Lukujoukot luonnollisista luvuista reaalilukuihin

Pro gradu -tutkielma
Esa Pulkka
517378
Itä-Suomen Yliopisto
Fysiikan ja matematiikan laitos
26. maaliskuuta 2012

Sisältö

1 Johdanto

Tässä pro gradu-tutkielmassa käymme läpi lukujoukkoja luonnollisista luvuista reaalilukuihin. Tarkastelemme niiden määritelmiä, ominaisuuksia sekä lyhyesti myös historiaa.

Määrittelemme ensin luonnolliset luvut ja niiden alkeelliset laskutoimitukset. Tämän jälkeen muodostamme kokonaislukujen joukon luonnollisten lukujen järjestettyjen parien avulla sekä tarkastelemme niihin liittyviä laskusääntöjä ja ominaisuuksia. Muodostamme rationaaliluvut saman tyyppisellä menetelmällä, kokonaislukujen järjestettyjä pareja käyttäen. Lopulta etenemme reaalilukujen tarkasteluun ja muodostamme reaalilukujen järjestelmän.

2 Luonnolliset luvut

Alkeellinen matematiikka alkoi luultavasti kun yritettiin vastata kysymyksiin kuten ”Kuinka montaa kalaa sait?”, ”Kuinka monta naista on luolassa?”, ”Kuinka monta päivää olet poissa?”. Pohjimmiltaan nämä kysymykset tarkoittavat ”Kuinka monta alkiota on tietyssä kohteiden (esine tai asia) ryhmässä tai joukossa?”. Vastatakseen tällaisiin kysymyksiin ihminen keksi luvut.

Yksinkertaiset luvut, kuten pienet luonnolliset luvut (1,2,3, ja niin edelleen), keksittiin epäilemättä ennen kirjoitettua historiaa. Myöhemmin, ehkä ei enempää kuin 2000 tai 3000 vuotta sitten, keksittiin luku nolla. Vaikka nämä luvut keksittiin ihmisten toimesta, niitä on käytetty niin kauan että olemme taipuvaisia ajattelemaan ikään kuin ne olisivat aina olleet olemassa. Kuitenkin varsinainen luonnollisten lukujen järjestelmä kyettiin muodostamaan joukko-opin ja logiikan pohjalle vasta 1800-luvulla ja sen ristiriitaisuudesta kiistellään vielä nykyaikanakin matemaatikkojen keskuudessa.

Luonnolliset luvut ovat arkipäiväisin lukujoukko. Ne kuvaavat asioiden tai esineiden lukumääriä. Nämä luvut olivat riittäviä ihmisen matemaattisten tarpeiden kannalta vuosituhansia. Luku nolla on tärkeä luonnollisten lukujen joukon tarkastelussa, vaikkakin sen ei kaikissa tarkasteluissa katsota kuuluvan luonnollisten lukujen joukkoon.

2.1 Luonnollisten lukujen määritelmä

Ensimmäisen luonnollisten lukujen aksiomaattisen määrittelyn esitti italialainen matemaatikko Giuseppe Peano vuonna 1889. Yksinkertaisiin käsitteisiin 0, S, $+$ ja $\cdot$ pohjautuvat Peanon aksioomat ovat:

(P1) Jos $S(n) = S(m)$, niin $n = m$;

(P2) $S(n) \neq 0$;

(P3) $n + 0 = n$;

(P4) $n + S(m) = S(n + m)$;

(P5) $n \cdot 0 = 0$;

(P6) $n \cdot S(m) = (n \cdot m) + n$;

(P7) Jos $n \neq 0$, niin $n = S(k)$ jollakin luvulla k ;

(P8) Induktiokaava. Olkoon A aritmeettinen ominaisuus (toisin sanoen ominaisuus, joka voidaan ilmaista merkinnöillä $+, \cdot, S, 0$). Jos luku 0 toteuttaa ominaisuuden A ja jos siitä, että $A(k)$ seuraa $A(S(k))$ kaikilla luvuilla k, niin jokaisella luvulla on ominaisuus A.

Kirjallisuudessa on useita eri versioita Peanon aksioomista. Edellä esitelty kahdeksanosainen versio on lähdeteoksesta [2].

Emme kuitenkaan tarkastele tässä tutkielmassa luonnollisia lukuja Peanon aksioomien pohjalta, vaan joukko-opin lähtökohdista. Aloitamme määrittelemällä induktiivisen joukon ja etenemme tätä kautta matemaatikko John von Neumannin vuonna 1923 luomaan luonnollisten lukujen määrittelyyn kirjaa The Number Systems Of Analysis [4] mukaillen.

Määritellään ensin induktiivinen joukko lähdeteoksen [2] mukaisesti.

Määritelmä 2.1.1. Joukko Y, jonka alkiot ovat joukkoja, on *induktiivinen* jos $\emptyset \in Y$ ja $X \cup \{X\} \in Y$ kaikilla $X \in Y$.

Perusolettamus tässä tarkastelussa on, että induktiivinen joukko on olemassa.

Lause 2.1.2. *On olemassa yksikäsitteinen induktiivinen joukko joka sisältyy jokaiseen induktiiviseen joukkoon.*

Todistus. Olkoon Z induktiivinen joukko ja olkoon Y kaikkien induktiivisten joukkoon Z sisältyvien joukkojen joukko. Määritellään $\mathbb{N} = \cap Y$. Osoitetaan, että $\mathbb{N}$ on tämä vaadittu joukko.

Ensin todistetaan, että $\mathbb{N}$ on jokaisen induktiivisen joukon osajoukko. Olkoon S induktiivinen joukko ja $n \in \mathbb{N}$. On huomattava, että $\emptyset \in Z \cap S$, sillä Z ja S ovat molemmat induktiivisia. Lisäksi jokaiselle $X \in Z \cap S$ pätee $X \in Z$ ja $X \in S$, joten $X \cup \{X\} \in Z \cap S$. Tästä johtuen $Z \cap S$ on joukon

Z induktiivinen osajoukko ja siten $Z \cap S \in Y$. Koska $\mathbb{N} = \cap Y$, seuraa että $\mathbb{N} \subseteq Z \cap S$. Erityisesti pätee $\mathbb{N} \subseteq S$.

Seuraavaksi osoitamme, että $\mathbb{N}$ on induktiivinen. Koska $\emptyset$ on jokaisen induktiivisen joukon alkio, on oltava $\emptyset \in \cap Y$. Näin ollen $\emptyset \in \mathbb{N}$. Olkoon $m \in \mathbb{N}$. Koska $\mathbb{N} \subseteq S$, on $m \in S$. Mutta S on induktiivinen, joten $m \cup \{m\} \in S$. Koska S on mielivaltainen induktiivinen joukko ja joukon Y joukot ovat induktiivisia, voidaan päätellä että $m \cup \{m\} \in \cap Y$. Siten $m \cup \{m\} \in \mathbb{N}$ ja päättelemme että $\mathbb{N}$ on induktiivinen.

Oletetaan, että M on induktiivinen joukko joka sisältyy jokaiseen induktiiviseen joukkoon. Tällöin $M \subseteq \mathbb{N}$ ja $\mathbb{N} \subseteq M$ ja niin $M = \mathbb{N}$. Siten $\mathbb{N}$ on yksikäsitteinen. □

Jatkossa käytämme merkintää $\mathbb{N}$ yksikäsitteiselle induktiiviselle joukolle joka sisältyy jokaiseen induktiiviseen joukkoon. Joukon $\mathbb{N}$ alkioita kutsutaan luonnollisiksi luvuiksi. Luonnollista lukua $\emptyset$ merkitään 1, luonnollista lukua $\emptyset \cup \{\emptyset\} = \{\emptyset\} = \{1\}$ merkitään 2 ja luonnollista lukua $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{1, 2\}$ merkitään 3. Kehitämme nyt luonnollisten lukujen alkeelliset ominaisuudet.

Jokaisella $n \in \mathbb{N}$ pätee $n \cup \{n\} \in \mathbb{N}$. Määritellään

$$S(n) = n \cup \{n\}$$

kaikilla $n \in \mathbb{N}$. Tällöin S on kuvaus $\mathbb{N} \to \mathbb{N}$. Luku $S(n)$ on luvun n *seuraaja*, ja sitä merkitään jatkossa myös n^+. Esimerkiksi $1^+ = 1 \cup \{1\} = \{1\} = 2$. Vastaavasti $2^+ = 2 \cup \{2\} = \{1\} \cup \{2\} = \{1, 2\} = 3$. Kuvaus S on *seuraaja-funktio*.

Siis luku 1 kuuluu luonnollisten lukujen joukkoon ja jokaiselle luvulle $n \in \mathbb{N}$ on määritetty, kuinka joukon $\mathbb{N}$ uusi jäsen n^+ muodostetaan. Todistaaksemme lauseen koskien jokaista lukua $n \in \mathbb{N}$, riittää muodostaa lause luvulle 1 ja sitten osoittaa että sama pätee myös arvolla n^+, aina kun se pätee tietyllä $n \in \mathbb{N}$. Tämä menetelmä on tehokas luonnollisten lukujen todistukseen ja sitä kutsutaan *induktioksi* (muuttajaan n kohdistuen). Oletusta, että lause pätee tietyllä luvulla n, kutsutaan *induktio-oletukseksi*.

Määrittelemme induktion täsmällisemmin lauseena.

Lause 2.1.3. *Olkoon M joukon $\mathbb{N}$ osajoukko siten, että $1 \in M$. Oletetaan myös, että $n^+ \in M$, aina kun $n \in M$. Tällöin $M = \mathbb{N}$.*

Todistus. Oletuksesta nähdään, että M on induktiivinen joukko. Joukko $\mathbb{N}$ sisältyy jokaiseen induktiiviseen joukkoon ja tästä voidaan päätellä, että $\mathbb{N} \subseteq M$. Mutta koska $M \subseteq \mathbb{N}$, niin on oltava $M = \mathbb{N}$. □

Induktion tekniikka voidaan nähdä erityistapauksena edelliselle lauseelle: Olkoon M kaikkien sellaisten luonnollisten lukujen joukko joille annettu väite

p pätee ja pyritään todistamaan, että p pätee kaikilla luonnollisilla luvuilla (toisin sanoen, että $M = \mathbb{N}$) osoittamalla että M toteuttaa lauseen oletukset.

Funktion *surjektiivisuus* tarkoittaa sitä, että jokaiseen maalijoukon alkioon voidaan liittää jokin lähtöjoukon alkio. Induktion sovelluksena todistamme seuraavassa lauseessa, että jokainen luonnollinen luku $n \neq 1$ on luonnollisen luvun seuraaja eli seuraajafunktio S on surjektio.

Lause 2.1.4. *Kuvaus S on surjektio joukosta $\mathbb{N}$ joukkoon $\mathbb{N} \setminus \{1\}$.*

Todistus. Olkoon $M = \{1\} \cup S(\mathbb{N})$. Siten $M \subseteq \mathbb{N}$ ja $1 \in M$. Seuraavaksi valitsemme $m \in M$. Koska $m^+ = S(m)$, pätee $m^+ \in S(\mathbb{N})$. Täten $m^+ \in M$. Induktioperiaatteen nojalla seuraa, että $\mathbb{N} = M = \{1\} \cup S(\mathbb{N})$. Koska $S(n) \neq \emptyset$ kaikilla $n \in \mathbb{N}$, pätee myös $1 \notin S(\mathbb{N})$. Tästä johtuen $S(\mathbb{N}) = \mathbb{N} \setminus \{1\}$, kuten oli osoitettava. □

Pitäisi vielä saada osoitettua, että S on *injektio*. Tämä tarkoittaa sitä, että jos m ja n ovat toisistaan eroavat luonnolliset luvut, niin $m^+ \neq n^+$. Tällöin olisi osoitettu, että jokainen luonnollinen luku, lukuunottamatta lukua 1, on yksikäsitteisen luonnollisen luvun seuraaja.

Injektiivisyyden perustelemista varten määrittelemme, että joukko Z (jonka alkiot ovat joukkoja) on *transitiivinen*, jos joukko X sisältyy joukkoon Z, aina kun on olemassa joukko Y siten, että $X \in Y$ ja $Y \in Z$. Täten jos Z on transitiivinen ja $Y \in Z$, pätee $X \in Z$ aina kun $X \in Y$. Näin ollen $Y \subseteq Z$. Käänteisesti, jos $Y \subseteq Z$, aina kun $Y \in Z$, niin Z on transitiivinen: Jos nimittäin $X \in Y$ ja $Y \in Z$, niin oletuksen mukaan $Y \subseteq Z$ ja siten $X \in Z$. Toisin sanoen joukko Z on transitiivinen jos ja vain jos jokainen alkio on joukon Z osajoukko.

Lemma 2.1.5. *Jokainen luonnollinen luku on transitiivinen.*

Todistus. Olkoon M transitiivisten luonnollisten lukujen joukko. Koska tyhjällä joukolla $\emptyset$ ei ole alkioita on selvää, että jokainen alkio on joukon $\emptyset$ osajoukko. Näin ollen $\emptyset$ on transitiivinen ja siten $1 \in M$. Olkoon $n \in M$. Täydennetään todistus induktiolla, osoittamalla että n^+ on transitiivinen. Olkoon $m \in n^+ = n \cup \{n\}$ ja $l \in m$. Osoittaaksemme että $m \subseteq n^+$, on todistettava että $l \in n^+$. On kaksi eri vaihtoehtoa: joko $m \in n$ tai $m \in \{n\}$. Aiemmassa tapauksessa on $l \in n$, koska n on transitiivinen. Toisessa tapauksessa $m = n$ ja siten $l \in n$. Molemmissa tapauksissa $l \in n^+$. Päädymme tulokseen, että $m \subseteq n^+$, joten n^+ on transitiivinen kuten oli osoitettava. □

Nyt voimme esittää halutun tuloksen.

Lause 2.1.6. *Seuraajafunktio S on injektio.*

Todistus. On rajattava pois vaihtoehto, että olisi olemassa erilliset luonnolliset luvut joille pätee $S(m) = S(n)$. Oletetaan tätä varten, että $m \cup \{m\} = n \cup \{n\}$ ja $m \neq n$. Koska $m \in m \cup \{m\} = n \cup \{n\}$, mutta $m \neq n$, on oltava $m \in n$. Lemman 2.1.5 mukaan n on transitiivinen ja siten $m \subseteq n$. Vastaava perustelu osoittaa, että $n \subseteq m$ josta seuraa ristiriita, että $m = n$ ja siten lause on todistettu. □

Lauseista 2.1.4 ja 2.1.6 seuraa, että jokainen luonnollinen luku $n \neq 1$ on yksikäsitteisen luonnollisen luvun seuraaja.

Lause 2.1.7. *Kaikilla $n \in \mathbb{N}$ pätee $n^+ \neq n$.*

Todistus. Koska $1^+ \neq \emptyset = 1$, lause pätee kun $n = 1$. Oletetaan induktio-oletuksena, että n on luonnollinen luku jolle lause pätee. Tällöin $n^+ \neq n$. Tästä johtuen Lauseen 2.1.6 nojalla $n^{++} \neq n^+$. Toisin sanoen, lause pätee arvolla n^+ ja siten lause on todistettu. □

Lauseesta 2.1.7 seuraa, että luonnollinen luku ei voi olla itsensä seuraaja. Edeltävät lauseet mahdollistavat luonnollisten lukujen listauksen sellaisessa järjestyksessä, että 1 on ensimmäisenä ja jokaista lukua seuraava luku on kyseisen luvun seuraaja.

Olkoon F kuvaus joukosta X joukkoon X. Olkoon lisäksi $x \in X$. Jossakin erityisessä tapauksessa saatamme haluta valita peräkkäiset joukon X alkiot alkaen alkiosta x ja soveltaa funktiota F toistuvasti. Tällainen valinta voidaan suorittaa muodostamalla funktio H joukosta $\mathbb{N}$ joukkoon X siten, että $H(1) = x$ ja kun H kuvaa luonnollisen luvun n alkioksi $y \in X$, niin H kuvaa arvon n^+ alkioksi $F(y)$. Toisin sanoen, $H(S(n)) = F(H(n))$ jokaisella $n \in \mathbb{N}$.

Intuitiivisesti tämä tarkoittaa, että H liittää luonnolliset luvut valitsemiimme joukon X alkioihin niin, että peräkkäiset luonnolliset luvut on liitetty peräkkäisiin valintoihin. Seuraavaa lausetta kutsutaan rekursiolauseeksi. Sen sisältö on, että tällainen yksikäsitteinen funktio H on olemassa.

Lause 2.1.8. *Olkoon $F : X \to X$ kuvaus ja olkoon $x \in X$. Tällöin on olemassa yksikäsitteinen kuvaus $H : \mathbb{N} \to X$ siten, että $H(1) = x$ ja $H \circ S = F \circ H$.*

Todistus. Määritämme $H = \cap T$, jossa T on kaikkien $W \subseteq \mathbb{N} \times X$ joukko, joka toteuttaa ehdot $(1, x) \in W$ ja $(n^+, F(y)) \in W$, kun $(n, y) \in W$. On todistettava, että H on funktio joukosta $\mathbb{N}$ joukkoon X. Ensin on kuitenkin osoitettava, että $T \neq \emptyset$. Tätä varten riittää todistaa, että $\mathbb{N} \times X \in T$.

Selvästi $\mathbb{N} \times X \subseteq \mathbb{N} \times X$ ja $(1, x) \in \mathbb{N} \times X$. Valitsemme $(n, y) \in \mathbb{N} \times X$. Tällöin $n \in \mathbb{N}$ ja $y \in X$. Siten $n^+ \in \mathbb{N}$ ja $F(y) \in X$ ja tästä seuraa, että

$(n^+, F(y)) \in \mathbb{N}\times X$. Tästä johtuen, joukon T määrittelyn mukaan, $\mathbb{N}\times X \in T$. Siten $T \neq \emptyset$.

Seuraavaksi osoitamme, että $H \in T$. Koska H on $\mathbb{N} \times X$ osajoukkojen leikkaus, selvästi $H \subseteq \mathbb{N} \times X$. Lisäksi $(1, x) \in H$, koska $T \neq \emptyset$ ja $(1, x) \in W$ kaikilla $W \in T$. Lopulta, jos $(n, y) \in H = \cap T$, niin $(n, y) \in W$ kaikilla $W \in T$. Tästä johtuen $(n^+, F(y)) \in W$ kaikilla $W \in T$ ja siten $(n^+, F(y)) \in \cap T = H$. Päädymme tulokseen $H \in T$.

Osoittaaksemme, että H on kuvaus joukosta $\mathbb{N}$ joukkoon X, on osoitettava, että jokaista $n \in \mathbb{N}$ vastaa yksikäsitteinen $a \in X$ jolle $(n, a) \in H$. Todistetaan tämä induktiolla muuttujan n suhteen.

On jo tiedossa, että $(1, x) \in H$. Oletetaan, että x ei ole joukon X ainoa alkio, jolla on tämä ominaisuus. Tällöin on olemassa $b \in X \setminus \{x\}$ siten, että $(1, b) \in H$. Määritellään $H_b = H \setminus \{(1, b)\}$. Todistetaan, että $H_b \in T$. Selvästi $H_b \subseteq H \subseteq \mathbb{N} \times X$ ja $(1, x) \in H_b$, koska $x \neq b$. Oletetaan, että $(n, y) \in H_b$. On osoitettava, että $(n^+, F(y)) \in H_b$. Koska $(n, y) \in H$ ja $H \in T$, saadaan $(n^+, F(y)) \in H$. Lisäksi $(n^+, F(y)) \neq (1, b)$, koska $n^+ \neq 1$ ja siksi $(n^+, F(y)) \in H \setminus \{(1, b)\} = H_b$. Tästä johtuen $H_b \in T$ ja päädymme ristiriitaan $H \subseteq H_b$, koska $H \subseteq W$ kaikilla $W \in T$. Johtopäätös tästä on, että luvun x on oltava yksikäsitteinen.

Valitaan nyt induktio-oletukseksi, että jollakin $n \in \mathbb{N}$ on olemassa yksikäsitteinen $a \in X$ siten, että $(n, a) \in H$. Koska $H \in T$, saadaan $(n^+, F(a)) \in H$. On osoitettava, että $F(a)$ on ainoa joukon X alkio jolla on tämä ominaisuus. Jos näin ei ole, on olemassa $c \in X \setminus \{F(a)\}$ siten, että $(n^+, c) \in H$. Määritellään $H_c = H \setminus \{(n^+, c)\}$.

Vahvistamme nyt, että $H_c \in T$. Selvästi $H_c \subset \mathbb{N} \times X$ ja $(1, x) \in H_C$, koska $n^+ \neq 1$. Valitaan $(m, z) \in H_c$. Osoitetaan, että $(m^+, F(z)) \in H_c$. Koska $(m, z) \in H_c \subseteq H$ ja $H \in T$, saadaan $(m^+, F(z)) \in H$. On rajattava pois mahdollisuus, että $(m^+, F(z)) = (n^+, c)$. Jos tämä yhtälö pätee, niin $m^+ = n^+$ ja $F(z) = c \neq F(a)$. Lause 2.1.6 osoittaa, että tuloksesta $m^+ = n^+$ seuraa $m = n$ siten, että $(n, z) \in H$. Toisaalta jälkimmäisestä tuloksesta eli siitä, että $F(z) = c \neq F(a))$ saadaan $z \neq a$. Tämä päätelmä on ristiriidassa alkion a yksikäsitteisyyden eli induktio-oletuksen kanssa. Tästä johtuen $(m^+, F(z)) \neq (n^+, c)$ ja siten $(m^+, F(z)) \in H \setminus \{(n^+, c)\} = H_c$. Olemme nyt todistaneet, että $H_c \in T$. Tästä seuraa ristiriita että $H \subseteq H_c$. Siten $F(a)$ on ainoa alkio $v \in X$ jolle $(n^+, v) \in H$. Olemme todistaneet induktiolla että H on funktio joukosta $\mathbb{N}$ joukkoon X. Lisäksi, $H(1) = x$ kun $(1, x) \in H$.

Seuraavaksi osoitamme, että $H \circ S = F \circ H$. Kaikilla $(n, y) \in H$ pätee $H(n) = y$ ja $(n^+, F(y)) \in H$. Siten $H(n^+) = F(y)$, joten

$$(H \circ S)(n) = H(S(n)) = H(n^+) = F(y) = F(H(n)) = (F \circ H)(n)$$

kaikilla $n \in \mathbb{N}$. Siis $H \circ S = F \circ H$.

On vielä osoitettava, että H on yksikäsitteinen. Olkoon G funktio joukosta $\mathbb{N}$ joukkoon X siten, että $G(1) = x$ ja $G \circ S = F \circ G$. Riittää osoittaa induktiolla, että $G(n) = H(n)$ kaikilla $n \in \mathbb{N}$. Selvästi $G(1) = x = H(1)$. Oletetaan induktio-oletuksena, että $G(n) = H(n)$ jollakin $n \in \mathbb{N}$. Tällöin

$$\begin{aligned} G(n^+) &= G(S(n)) = (G \circ S)(n) = (F \circ G)(n) \\ &= F(G(n)) = F(H(n)) = (F \circ H)(n) \\ &= (H \circ S)(n) = H(S(n)) = H(n^+). \end{aligned}$$

Näin ollen induktioperiaatteen nojalla $G(n) = H(n)$ kaikilla $n \in \mathbb{N}$ ja siten $G = H$. On todistettu, että H on yksikäsitteinen. □

Olkoon X joukko. *Binäärinen laskutoimitus* samassa joukossa on kuvaus joukosta $X \times X$ joukkoon X. Täten binäärioperaatio kuvaa jokaisen luonnollisten lukujen järjestetyn parin yksikäsitteiselle luonnolliselle luvulle. Seuraava rekursiolauseen sovellus mahdollistaa binäärioperaatioiden esittelyn joukossa $\mathbb{N}$.

Lause 2.1.9. *Olkoot $F, F_m : \mathbb{N} \to \mathbb{N}$, kuvauksia missä $m \in \mathbb{N}$. Tällöin on olemassa yksikäsitteinen binäärioperaatio H joukossa $\mathbb{N}$ siten, että*

$$H(m, 1) = F(m)$$

kaikilla $m \in \mathbb{N}$ ja

$$H(m, n^+) = F_m(H(m, n))$$

kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$.

Todistus. Todistetaan ensin funktion H olemassaolo. Olkoon $m \in \mathbb{N}$. Rekursiolauseen mukaan (sovellettuna kuvaukseen F_m joukossa $\mathbb{N}$ kun $x = F(m)$), on olemassa yksikäsitteinen kuvaus $H_m : \mathbb{N} \to \mathbb{N}$ jolle pätee $H_m(1) = F(m)$ ja $H_m \circ S = F_m \circ H_m$. Kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$ määritetään $H(m, n) = H_m(n)$. Tällöin

$$H(m, 1) = H_m(1) = F(m)$$

ja

$$\begin{aligned} H(m, n^+) &= H(n^+) = H_m(S(n)) = (H_m \circ S)(n) \\ &= (F_m \circ H_m)(n) = F_m(H_m(n)) = F_m(H(m, n)), \end{aligned}$$

kuten vaadittiin.

Olkoon G binäärioperaatio joukossa $\mathbb{N}$ siten, että $G(m,1) = F(m)$ kaikilla $m \in \mathbb{N}$ ja $G(m,n^+) = F_m(G(m,n))$ kaikilla $(m,n) \in \mathbb{N}\times\mathbb{N}$. Osoittaaksemme funktion H yksikäsitteisyyden, on osoitettava, että $H = G$. Riittää osoittaa, että $H(m,n) = G(m,n)$ kaikilla $(m,n) \in \mathbb{N}\times\mathbb{N}$. Valitaan $m \in \mathbb{N}$. Todistetaan induktiolla muuttujan n suhteen, että $H(m,n) = G(m,n)$ kaikilla $n \in \mathbb{N}$. Selvästi $H(m,1) = F(m) = G(m,1)$. Oletetaan induktio-oletuksena, että $H(m,n) = G(m,n)$ jollakin luvulla $n \in \mathbb{N}$. Tällöin

$$H(m,n^+) = F_m(H(m,n)) = F_m(G(m,n)) = G(m,n^+),$$

kuten pitikin ja näin ollen $H = G$. □

Funktio H määrittää miten luku $m \in \mathbb{N}$ tulee yhdistetyksi muihin luonnollisiin lukuihin määritellen binäärioperaation joukossa $\mathbb{N}$. Seuraavissa osissa annamme kolme esimerkkiä, joista saadaan binäärioperaatiot, joita kutsutaan erikseen yhteenlaskuksi, kertolaskuksi ja potenssiinkorotukseksi.

2.2 Luonnollisten lukujen ominaisuuksia

Lause 2.2.1. *On olemassa binäärioperaatio H luonnollisten lukujen joukossa $\mathbb{N}$, jolle pätee*

$$H(m,1) = m^+$$

kaikilla $m \in \mathbb{N}$ ja

$$H(m,n^+) = (H(m,n))^+$$

kaikilla $(m,n) \in \mathbb{N}\times\mathbb{N}$.

Todistus. Sovelletaan Lausetta 2.1.9 valitsemalla $F_m = F = S$ kaikilla $m \in \mathbb{N}$. □

Perusteluna yhtälölle $H(m,n^+) = (H(m,n))^+$ on se, että alkioiden m ja n^+ yhteenlaskusta täytyy saada tulokseksi seuraaja luonnolliselle luvulle, joka saadaan lukujen m ja n yhteenlaskusta.

Binäärioperaatiota H, joka määriteltiin edellä, nimitetään *yhteenlaskuksi* ja lukua $H(m,n)$ kutsutaan luonnollisten lukujen m ja n *summaksi*. Yleisesti kirjoitamme $m+n$ merkinnän $H(m,n)$ sijaan. Tällä tavoin merkittynä edellisen lauseen yhtälöt voidaan kirjoittaa

$$m^+ = m+1$$

kaikilla $m \in \mathbb{N}$ sekä

$$m+(n+1) = m+n^+ = (m+n)^+ = (m+n)+1$$

kaikilla $m \in \mathbb{N}$ ja $n \in \mathbb{N}$.

Etenemme tarkastelemaan tämän laskutoimituksen perusominaisuuksia. Ensimmäinen tällainen ominaisuus on *assosiatiivisuus* eli *liitännäisyys*.

Lause 2.2.2. *Jos* $(k, m, n) \in \mathbb{N} \times \mathbb{N}$*, niin*

$$k + (m + n) = (k + m) + n.$$

Todistus. Tiedetään, että tulos pätee kun $n = 1$. Oletetaan, että k ja m ovat kiinnitettyjä luonnollisia lukuja, sekä induktio-oletuksena, että lause pätee jollakin $n \in \mathbb{N}$. Saadaan

$$\begin{aligned} k + (m + (n + 1)) &= k + ((m + n) + 1) \\ &= (k + (m + n)) + 1 \\ &= ((k + m) + n) + 1 \\ &= (k + m) + (n + 1). \end{aligned}$$

Lause seuraa induktioperiaatteesta. □

Tavallisesti kirjoitamme $k + m + n$ sen sijaan, että kirjoittaisimme $k + (m + n)$. Esimerkkinä

$$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 3 + 1 = 4.$$

Kommutatiivisuus eli *vaihdannaisuus* pätee myös. Todistetaan väite ensin erityistapauksessa.

Lemma 2.2.3. *Jos* $n \in \mathbb{N}$ *, niin* $n + 1 = 1 + n$.

Todistus. Lemma pätee selvästi kun $n = 1$. Oletetaan induktio-oletuksena, että $n + 1 = 1 + n$ jollakin arvolla $n \in \mathbb{N}$. Tällöin

$$(n + 1) + 1 = (1 + n) + 1 = 1 + (n + 1)$$

liitännäisyyden nojalla. Lemma seuraa induktioperiaatteesta. □

Seuraavaksi voimme esittää luonnollisten lukujen yhteenlaskun vaihdannaisuuden.

Lause 2.2.4. *Jos* $(m, n) \in \mathbb{N} \times \mathbb{N}$*, niin* $m + n = n + m$.

Todistus. Käytetään induktiota muuttujan n suhteen. Edellä olevan Lemman 2.2.3 mukaan lause pätee, kun $n = 1$. Oletetaan induktio-oletuksena, että $m + n = n + m$ jollakin $n \in \mathbb{N}$. Tällöin

$$\begin{aligned} m + (n + 1) &= (m + n) + 1 = (n + m) + 1 \\ &= n + (m + 1) = n + (1 + m) \\ &= (n + 1) + m. \end{aligned}$$

Lause seuraa induktioperiaatteesta. □

Seuraavaa laskusääntöä kutsutaan *supistussäännöksi.*

Lause 2.2.5. *Jos* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *ja* $k + n = m + n$*, niin* $k = m$*.*

Todistus. Käytetään induktiota muuttujan n suhteen. Kun $n = 1$, lause seuraa välittömästi siitä, että seuraajafunktio S on injektio. Oletetaan induktio-oletuksena, että lause pätee jollakin $n \in \mathbb{N}$. Osoitetaan, että

$$k + n + 1 = m + n + 1.$$

Jälleen koska S on injektio, niin $k + n = m + n$ ja tästä seuraa induktio-oletuksen mukaan $k = m$. Täten lause pätee induktioperiaatteen nojalla. □

Lause 2.2.6. *Jos* $(m, n) \in \mathbb{N} \times \mathbb{N}$*, niin* $n \neq m + n$*.*

Todistus. Väittämä pätee arvolla $n = 1$, koska $1 \notin S(\mathbb{N})$. Olkoon $m \in \mathbb{N}$ ja oletetaan, että $n \neq m + n$ jollakin $n \in \mathbb{N}$. Tällöin $n + 1 \neq m + n + 1$, koska S on injektio ja täten lause seuraa induktioperiaatteen nojalla. □

Seuraava tarkasteltava laskutoimitus on kertolasku.

Lause 2.2.7. *On olemassa yksikäsitteinen binäärioperaatio* H *joukossa* $\mathbb{N}$ *siten, että*

$$H(m, 1) = m$$

kaikilla $m \in \mathbb{N}$ *ja*

$$H(m, n^+) = H(m, n) + m$$

kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$*.*

Todistus. Sovelletaan Lausetta 2.1.9 valitsemalla $F = I_{\mathbb{N}}$ ja $F_m(n) = n + m$ kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$. □

Perustelu yhtälölle $H(m, n^+) = H(m, n) + m$ on se, että lukujen m ja $n^+ = n + 1$ kertolaskusta täytyy saada sama luku, kuin joka saadaan laskemalla yhteen lukujen m ja n kertolaskun tulos ja luku m. Kertolasku on karkeasti ilmaistuna siis lyhennystapa toistetulle yhteenlaskulle.

Tätä binäärioperaatiota kutsutaan *kertolaskuksi* ja lukua $H(m, n)$ kutsutaan luonnollisten lukujen m ja n *tuloksi.* Yleisesti kirjoitamme $m \cdot n$, tai

yksinkertaisesti mn sen sijaan, että merkitsisimme $H(m, n)$. Voidaan siis kirjoittaa

$$m \cdot 1 = m$$

kaikilla $m \in \mathbb{N}$ ja

$$m(n + 1) = mn + m$$

kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$. Kertolasku on laskujärjestyksessä etusijalla yhteenlaskuun nähden. Esimerkiksi

$$2 \cdot 2 = 2 \cdot (1 + 1) = 2 \cdot 1 + 2 = 2 + 2 = 4.$$

Seuraava lause osoittaa, että kertolasku on *distributiivinen* eli seuraava *osittelulaiksi* kutsuttu ominaisuus on sille voimassa.

Lause 2.2.8. *Jos* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$*, niin*

$$(k + m)n = kn + mn.$$

Todistus. Käytetään induktiota muuttujan n suhteen. Lause pätee arvolla $n = 1$, sillä

$$(k + m) \cdot 1 = k + m = k \cdot 1 + m \cdot 1.$$

Oletetaan induktio-oletuksena, että on olemassa $n \in \mathbb{N}$ jolla lause pätee. Tällöin

$$\begin{aligned}
(k + m)(n + 1) &= (k + m)n + k + m \\
&= (kn + mn) + (k + m) \\
&= ((kn + mn) + k) + m \\
&= (kn + (mn + k)) + m \\
&= (kn + (k + mn)) + m \\
&= ((kn + k) + mn) + m \\
&= (kn + k) + (mn + m) \\
&= k(n + 1) + m(n + 1).
\end{aligned}$$

Induktioperiaatteen nojalla lause on todistettu. □

Osoitamme vaihdannaisuuden todistamalla erityistapauksen ensin.

Lemma 2.2.9. *Kaikilla* $n \in \mathbb{N}$ *pätee* $1 \cdot n = n \cdot 1$.

Todistus. Lemma on triviaali arvolla $n = 1$. Oletetaan, että $1 \cdot n = n \cdot 1$ pätee jollakin arvolla $n \in \mathbb{N}$. Tällöin

$$1 \cdot (n+1) = 1 \cdot n + 1 = n \cdot 1 + 1 = n + 1 = (n+1) \cdot 1,$$

kuten oli osoitettava. Täten induktioperiaatteen nojalla lemma on todistettu. □

Lause 2.2.10. *Jos* $(m, n) \in \mathbb{N} \times \mathbb{N}$*, niin* $mn = nm$*.*

Todistus. Edeltävän lemman mukaan lause pätee kun $n = 1$. Kiinnitetään m ja oletetaan, että $mn = nm$ jollakin valinnalla $n \in \mathbb{N}$. Tällöin

$$\begin{aligned} m(n+1) &= mn + m = mn + m \cdot 1 \\ &= nm + 1 \cdot m = (n+1)m. \end{aligned}$$

Induktioperiaatteen nojalla lause on todistettu. □

Kertolasku on myös liitännäinen.

Lause 2.2.11. *Jos* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$*, niin* $k(mn) = (km)n$*.*

Todistus. Olkoon $k \in \mathbb{N}$ ja $m \in \mathbb{N}$. Käytetään induktiota luvun n suhteen. Lause pätee kun $n = 1$, sillä

$$k(m \cdot 1) = km = (km) \cdot 1.$$

Nyt oletamme induktio-oletuksena, että $k(mn) = (km)n$ jollakin $n \in \mathbb{N}$. Tällöin

$$\begin{aligned} k(m(n+1)) &= k(mn + m) = k(mn) + km \\ &= (km)n + km = (km)(n+1) \end{aligned}$$

Lauseen 2.1.3 nojalla. □

Lause 2.2.12. *On olemassa yksikäsitteinen binäärioperaatio* H *luonnollisten lukujen joukossa* $\mathbb{N}$ *jolle*

$$H(m, 1) = m$$

kaikilla $m \in \mathbb{N}$ *ja*

$$H(m, n^+) = mH(m, n)$$

kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$*.*

Todistus. Sovelletaan Lausetta 2.1.9, valitaan $F = I_{\mathbb{N}}$ ja $F_m(n) = mn$ kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$. □

Tämä binäärioperaatio on nimeltään *potenssiin korotus* ja $H(m, n)$ kutsutaan luvun m *kertaluvun* n *potenssiksi*. Yleisesti kirjoitamme m^n merkinnän $H(m, n)$ sijaan. Näin ollen

$$m^1 = m$$

kaikilla $m \in \mathbb{N}$ ja

$$m^{n+1} = m \cdot m^n$$

kaikilla $(m, n) \in \mathbb{N} \times \mathbb{N}$.

Potenssiin korotus liittyy kertolaskuun samalla tavoin kuin kertolasku liittyy yhteenlaskuun. Esimerkiksi

$$2^2 = 2^{1+1} = 2 \cdot 2^1 = 2 \cdot 2 = 4.$$

On huomattavaa, että $1^1 = 1$ ja jos $1^n = 1$ jollakin $n \in \mathbb{N}$, niin tällöin

$$1^{n+1} = 1 \cdot 1^n = 1 \cdot 1 = 1.$$

Näin ollen $1^n = 1$ kaikilla $n \in \mathbb{N}$ induktioperiaatteen nojalla.

Etenemme potenssiin korotuksen alkeisominaisuuksiin. Ensimmäinen näistä on distributiivisuus kertolaskun suhteen.

Lause 2.2.13. *Kaikilla* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *pätee*

$$(km)^n = k^n m^n.$$

Todistus. Lause pätee arvolla $n = 1$, sillä

$$k^1 m^1 = km = (km) = (km)^1.$$

Asetetaan nyt $k \in \mathbb{N}$ ja $m \in \mathbb{N}$ ja oletetaan, että $(km)^n = k^n m^n$ jollakin $n \in \mathbb{N}$. Tällöin

$$k^{n+1} m^{n+1} = k^n k^1 m^n m^1 = k^n m^n k^1 m^1 = (km)^n (km)^1 = (km)^{n+1}.$$

Täten induktioperiaatteen nojalla lause on todistettu. □

Lause 2.2.14. *Kaikilla* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *pätee*

$$k^m k^n = k^{m+n}.$$

Todistus. Lause pätee arvolla $n = 1$, sillä

$$k^{m+1} = k^m k = k^m k^1.$$

Asetetaan nyt $k \in \mathbb{N}$ ja $m \in \mathbb{N}$ sekä oletetaan, että $k^m k^n = k^{m+n}$ jollakin $n \in \mathbb{N}$. Tällöin

$$k^{m+n+1} = k^{m+n} k = k^m k^n k = k^m k^{n+1}.$$

Täten induktioperiaatteen nojalla lause on todistettu. □

Lause 2.2.15. *Kaikilla* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *pätee*

$$(k^m)^n = k^{mn}.$$

Todistus. Lause pätee selvästi, kun $n = 1$. Asetetaan $k \in \mathbb{N}$ ja $m \in \mathbb{N}$ ja oletetaan, että $(k^m)^n = k^{mn}$ jollakin $n \in \mathbb{N}$. Tällöin

$$\begin{aligned}(k^m)^{n+1} &= (k^m)^n k^m = k^{mn} k^m \\ &= k^{mn+m} = k^{m(n+1)}.\end{aligned}$$

ja täten väittämä on todistettu induktioperiaatteen nojalla. □

Olkoon $m \in \mathbb{N}$ ja $n \in \mathbb{N}$. Sanotaan, että m on *pienempi kuin* n, tai n on *suurempi kuin* m, jos on olemassa $k \in \mathbb{N}$ siten, että $m + k = n$. Tässä tapauksessa voidaan kirjoittaa $m < n$ tai $n > m$. Kaikkien lukuparien $(m, n) \in \mathbb{N} \times \mathbb{N}$ joukko joille pätee $m < n$ määrittelee relaation joukossa $\mathbb{N}$. Tarkastelemme seuraavaksi tämän relaation ominaisuuksia.

Lause 2.2.16. *Jos* $k < m$ *ja* $m < n$*, niin* $k < n$*.*

Todistus. On olemassa $x \in \mathbb{N}$, jolla pätee $k + x = m$ ja $y \in \mathbb{N}$ jolla pätee $m + y = n$. Näin ollen $k + x + y = n$, joten $k < n$. □

Lause 2.2.17. *Olkoon* $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$*. Tällöin* $m < n$ *jos ja vain jos* $m + k < n + k$*.*

Todistus. Jos $m < n$, niin $n = m + l$ jollakin $l \in \mathbb{N}$. Tästä johtuen $m + k + l = n + k$ ja siten $m + k < n + k$. Kääntäen oletetaan, että $m + k < n + k$. Tällöin jollakin $l \in \mathbb{N}$ pätee $m + k + l = n + k$. Tästä saadaan $m + l = n$ eli $m < n$. □

Toisin sanoen sama luonnollinen luku voidaan lisätä epäyhtälön molemmille puolille.

Lauseesta 2.2.17 seuraa muutamia huomionarvoisia seikkoja. Pätee $m \leq n$ jos ja vain jos $m + k \leq n + k$ kaikilla $n \in \mathbb{N}$. Lisäksi jos $k < l$ ja $m < n$, niin

$$k + m < k + n < l + n.$$

Tästä seuraa, että jos $k < l$ ja $m \leq n$, niin $k + m < l + n$. Vastaavasti tämä epäyhtälö pätee, jos $k \leq l$ ja $m < n$. Näin ollen jos $k \leq l$ ja $m \leq n$, niin pätee $k + m \leq l + n$. Itse asiassa jos $k = l$ ja $m = n$, niin $k + m = l + n$. Jos näin ei olisi, niin $k + m < l + n$. Lisäksi jos $m < n$, niin tällöin on olemassa $k \in \mathbb{N}$ siten, että $m + k = n$. Koska $1 \leq k$, seuraa $m + 1 \leq n$. Täten jos $m + 1 > n$, niin $m \geq n$.

Lause 2.2.18. *Olkoon $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Tällöin $m < n$ jos ja vain jos $km < kn$.*

Todistus. Jos $m < n$, niin $n = m + l$ jollakin $l \in \mathbb{N}$. Tästä johtuen $kn = km + kl$ ja siten $km < kn$. Kääntäen oletetaan, että $km < kn$. Jos $m = n$, niin $km = kn$ ja jos $n < m$, niin $kn < km$. Molemmat näistä yhtälöistä on ristiriidassa oletuksen kanssa. Siten $m < n$. □

Lauseesta 2.2.18 seuraa suoraan että jos $km = kn$, niin $m = n$, sillä muuten päädytään ristiriitaan. Seuraa myös, että $m \leq n$ jos ja vain jos $km \leq kn$. Jos $k < l$ ja $m < n$, niin $km < kn < ln$. Näin ollen, jos $k < l$ ja $m \leq n$, niin $km < ln$. Samoin $km < ln$, jos $k \leq l$ ja $m < n$. Tästä johtuen, jos $k \leq l$ ja $m \leq n$, niin $km \leq ln$.

Lause 2.2.19. *Jos $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, niin $k^n < m^n$ jos ja vain jos $k < m$.*

Todistus. Oletetaan, että $k < m$. Käytetään induktiota muuttujan n suhteen. Ei ole todistettavaa jos $n = 1$. Oletetaan induktio-oletuksena, että $k^n < m^n$ jollakin $n \in \mathbb{N}$. Tällöin

$$k^{n+1} = k \cdot k^n < m \cdot m^m = m^{n+1},$$

ja niin $k^n < m^n$ yleisesti induktioperiaatteen nojalla. Kääntäen, jos $k^n < m^n$, niin $k < m$ koska toiset vaihtoehdot ovat ristiriidassa oletuksen kanssa. □

Lause 2.2.20. *Olkoon $(k, m, n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Tällöin $k^m < k^n$ jos ja vain jos $k > 1$ ja $m < n$.*

Todistus. Oletetaan, että $k > 1$ ja $m < n$. Tällöin $n = m + l$ jollakin $l \in \mathbb{N}$. Lisäksi $1 = 1^l < k^l$ ja siten

$$k^m = k^m \cdot 1 < k^m k^l = k^{m+l} = k^n.$$

Kääntäen, jos $k^m < k^n$, niin $k > 1$ koska $1^m = 1^n = 1$. Tästä voidaan päätellä, että $m < n$ koska muut vaihtoehdot ovat ristiriidassa oletuksen kanssa. □

Esimerkiksi jos $k > 1$ ja $n > 1$, niin $k^n > k$.

Olkoon $M \subseteq \mathbb{N}$. Jos $m \leq n$ jokaisella $n \in M$, niin lukua $m \in M$ kutsutaan joukon M *minimialkioksi* tai *minimiksi* ja merkitään $m = \min\{M\}$. Selvästi m on yksikäsitteinen, sillä jos $m \leq n$ ja $k \leq n$ kaikilla $n \in M$, missä $m \in M$ ja $k \in M$, niin $m \leq k$ ja $k \leq m$. Tällöin $m = k$. Vastaavasti lukua m kutsutaan *maksimiksi* joukossa M ja merkitään $m = \max\{M\}$, jos $m \geq n$ jokaisella $n \in M$.

Lause 2.2.21. *Olkoon $M \subseteq \mathbb{N}$ ja $M \neq \emptyset$. Tällöin joukossa M on pienin alkio eli minimi.*

Todistus. Olkoon K kaikkien sellaisten alkioiden $k \in \mathbb{N}$ joukko, joille $k \leq m$ kaikilla $m \in M$. Siten $1 \in K$ ja $K \neq \mathbb{N}$, sillä jos valitsemme $m \in M$, niin $m + 1 \notin K$, koska $m < m + 1$. Tästä johtuen on olemassa $k \in K$ siten, että $k + 1 \notin K$, koska muuten induktion nojalla olisi $K = \mathbb{N}$.

Muistetaan, että $k \leq m$ kaikilla $m \in M$. Osoittaaksemme, että k on joukon M minimialkio, on vielä näytettävä, että $k \in M$. Muuten $k < m$ kaikilla $m \in M$. Näin ollen $k+1 \leq m$ kaikilla $m \in M$ ja siten syntyy ristiriita, että $k + 1 \in K$. Tästä johtuen $k \in M$ ja k on joukon M minimialkio. □

Nyt voimme muodostaa vahvemman version induktioperiaatteesta.

Lause 2.2.22. *Olkoon $M \subseteq \mathbb{N}$. Oletetaan, että M sisältää jokaisen sellaisen luonnollisen luvun n, jolle $m \in M$ kaikilla luonnollisilla luvuilla $m < n$. Tällöin $M = \mathbb{N}$.*

Todistus. Oletetaan, että $M \neq \mathbb{N}$. Tällöin $\mathbb{N} \setminus M \neq \emptyset$. Edellisen Lauseen 2.2.21 nojalla, $\mathbb{N} \setminus M$ sisältää pienimmän eli minimialkion n. Kaikilla $m < n$ seuraa, että $m \notin \mathbb{N} \setminus M$, joten $m \in M$. Tästä johtuen oletuksesta seuraa ristiriita, että $n \in M$ ja niin voidaan päätellä, että $M = \mathbb{N}$. □

Lauseesta 2.2.22 seuraa, että todistaaksemme luonnollisiin lukuihin liittyvän lauseen riittää osoittaa, että lause pätee luonnollisella luvulla n, kun se pätee jokaisella luonnollisella luvulla joka on pienempi kuin n. Olettamus, että lause pätee jokaisella lukua n pienemmällä luonnollisella luvulla on tehokkaampi kuin aiemmin käytetty induktion periaate, täten tämä versio induktioperiaatteesta on myös tehokkaampi.

3 Kokonaisluvut

Jos lukio-opiskelijalla on 100 euroa rahaa ja hän kuluttaa 105 euroa, mikä on hänen nettovarallisuutensa? Luultavasti rahan ollessa kyseessä sanoisimme, että hänellä on 5 euroa velkaa. Jotta voisimme määrittää vastauksen matemaattisesti täsmällisesti, on välttämätöntä löytää luku joka vastaa tulosta $100 - 105$. Kuitenkin, koska $100 < 105$, ei luonnollisissa luvuissa ole sellaista lukua k jolle $100 = 105 + k$. Tässä tapauksessa vähennyslasku on mahdoton ilman luonnollisten lukujen joukon laajennusta.

On myös lukemattomia muita jokapäiväisiä esimerkkejä, jotka osoittavat tämän tarpeen. Oletetaan, että lämpötila on 10 astetta. Mikä on uusi lämpötila, jos lämpötila laskee 15 astetta? Vastaus voisi olla ”5 alle 0” tai ”5 vähemmän kuin 0”. Tämän tyyppisessä tilanteessa parhaalta ratkaisulta tuntuu keksiä uusia lukuja ja näin teemmekin. Kuvataksemme lukua ”10 vähemmän kuin 0”, käytämme symbolia -10. Voimme nyt ilmaista, että lämpötila on -10 astetta.

Kuten monien muidenkin uusien käsitteiden kanssa, negatiivisia lukuja ei suoraan hyväksytty edes matemaatikkojen toimesta. Diofantos Aleksandrialainen (noin vuonna 250) kutsui yhtälöä ”absurdiksi” mikäli sen ratkaisut olivat negatiivisia lukuja. Vasta noin 1600-luvulla negatiiviset luvut hyväksyttiin yleisesti oikeiksi luvuiksi.

Vähennyslaskua ei voida suorittaa rajoituksetta luonnollisten lukujen määrittelyjoukossa. Historiaa tarkastellen negatiivisia lukuja käsiteltiin aluksi varovasti juurien ja imaginaarilukujen tapaan aivan kuin ne olisivat fiktiivisiä ilmaisuja. Koulussa negatiiviset luvut esitetään usein lukusuoran avulla. Lukusuoralla luku 0 sijoitetaan origoon, luku 1 mittayksikön päähän oikealle, luku 2 mittayksikön päähän oikealle luvusta 1 ja niin edelleen. Negatiiviset luvut sijoitetaan vastaavalla tavalla origon vasemmalle puolelle.

Näin saatu lukujoukko, jota kutsutaan kokonaislukujen joukoksi, on luonnollisten lukujen laajennus ja se koostuu luonnollisista luvuista sekä luvuista jotka ovat muotoa $-n$, missä $n \in \mathbb{N}$ eli toisin sanoen negatiivisista luvuista. Algebrallisesti on kyse luonnollisten lukujen muodostaman additiivisen puoliryhmän laajentamisesta kokonaislukuihin. Kokonaislukujen määrittelyn pareina joukosta $\mathbb{N} \times \mathbb{N}$, jota seuraavana tarkastelemme, esitti ensimmäisenä saksalainen matemaatikko Richard Dedekind. Tämän luvun runkona on käytetty lähdeteoksia [4] ja [3].

3.1 Kokonaislukujen määritelmä

Jos m ja n ovat luonnollisia lukuja ja $m < n$, tällöin on olemassa luku $l \in \mathbb{N}$ siten, että $m + l = n$. Tämä luku l voidaan ilmaista $n - m$. Siten

$m + (n - m) = n$. Toisaalta ei ole olemassa luonnollista lukua l jolle pätee $1+l = 1$, koska $1 \notin S(\mathbb{N})$. Lisäksi jos $m > 1$, niin voidaan kirjoittaa $m = k+1$ jollakin $k \in \mathbb{N}$. Tästä johtuen ei voi olla olemassa luonnollista lukua l jolle $m + l = 1$, muuten olisi ristiriita $1 + k + l = 1$.

Nämä seikat johtavat tarkastelemaan muita lukuja luonnollisten lukujen sijaan. Ideana on määritellä uudenlainen luku, joka on joukko luonnollisten lukujen järjestettyjä pareja. Määritellään ensin ekvivalenssirelaation ja ekvivalenssiluokan käsitteet, joita tullaan tarvitsemaan kokonaislukujen määrittelemiseksi.

Määritelmä 3.1.1. Olkoon $\sim$ relaatio joukossa A. Relaation $\sim$ sanotaan olevan *ekvivalenssirelaatio*, mikäli se on refleksiivinen, symmetrinen ja transitiivinen joukossa A.

Relaatio $\sim$ joukossa A on refleksiivinen, mikäli kaikilla $a \in A$ pätee $a \sim a$. Symmetrisyys taasen tarkoittaa, että relaatiosta $a \sim b$ seuraa $b \sim a$. Transitiivisuus tarkoittaa, että kaikilla $a, b, c \in A$ ehdosta $a \sim b$ ja $b \sim c$ seuraa $a \sim c$. Kun nämä kolme ehtoa täyttyy, on relaatio ekvivalenssirelaatio.

Käsittelemme tässä tutkielmassa lukujoukkoja ja lukuja. Tarkastellaan kuitenkin havainnollistavaa esimerkkiä lukujen ulkopuolelta, joka on esitetty lähdeteoksessa [2], liittyen ekvivalenssiluokkiin. Olkoon P kaikkien maailman ihmisten joukko. Jos henkilö p asuu samassa maassa kuin henkilö q, merkitään $p \equiv q$ ja kutsutaan heitä ekvivalenteiksi. Varsin triviaalisti relaatio $\equiv$ on refleksiivinen, symmetrinen ja transitiivinen joukossa P. On huomattava, että P voidaan jakaa sisäisesti ekvivalentteihin alkioihin. Kaikki henkilöt jotka asuvat Yhdysvalloissa muodostavat yhden luokan, kaikki henkilöt Ranskassa toisen luokan ja niin edelleen. Kaikki saman luokan jäsenet ovat keskenään ekvivalentteja, toisaalta kahden eri luokan jäsenet eivät ole koskaan keskenään ekvivalentteja. Ekvivalenssiluokat vertautuvat tässä suoraan eri maihin.

Määritelmä 3.1.2. Olkoon $\sim$ ekvivalenssirelaatio joukossa A ja $a \in A$. Alkion a *ekvivalenssiluokka* on joukko

$$[a] = \{x \in A | x \sim a\}.$$

Jokainen ekvivalenssiluokka muodostuu keskenään ekvivalenteista alkioista, toisin sanoen a ja b kuuluvat samaan ekvivalenssiluokkaan jos ja vain jos $a \sim b$.

Määritellään ekvivalenssirelaatio joukossa $\mathbb{N} \times \mathbb{N}$. Jos $(k, l) \in \mathbb{N} \times \mathbb{N}$ ja $(m, n) \in \mathbb{N} \times \mathbb{N}$, merkitään

$$(k, l) \sim (m, n) \Leftrightarrow k + n = l + m.$$

Esimerkiksi $(3,1) \sim (4,2)$ ja $(4,2) \sim (5,3)$, sillä $3+2 = 1+4 = 5$ ja $4+3 = 2+5 = 7$. Jos $(k,l) \sim (m,n)$ ja $m > n$, seuraa $l < k$. Lisäksi

$$l + (k-l) + n = k + n = l + m = l + n + (m-n),$$

ja siten Lauseen 2.2.5 nojalla $k-l = m-n$. Yleisesti, jos $(k,m,n) \in \mathbb{N}\times\mathbb{N}\times\mathbb{N}$, niin $(m,n) \sim (m+k, n+k)$ sillä $m+n+k = n+m+k$.

Lause 3.1.3. *Relaatio* $\sim$ *on ekvivalenssirelaatio joukossa* $\mathbb{N} \times \mathbb{N}$.

Todistus. Suoraan yhteenlaskun kommutatiivisuudesta seuraa, että $(m,n) \sim (m,n)$ kaikilla $(m,n) \in \mathbb{N} \times \mathbb{N}$. Toisin sanoen, refleksiivisyys pätee. Symmetrisyys seuraa samoin yhtäsuuruuden symmetrisyydestä ja yhteenlaskun kommutatiivisuudesta. Oletetaan, että $(i,j) \sim (k,l)$ ja $(k,l) \sim (m,n)$. Tällöin $i+l = j+k$ ja $k+n = l+m$. Siten

$$i + l + k + n = j + k + l + m$$

ja tästä seuraa Lauseen 2.2.5 mukaan $i+n = j+m$. Toisin sanoen $(i,j) \sim (m,n)$ ja transitiivisuus on siten todistettu. □

Olkoon $\mathbb{Z}$ relaation $\sim$ ekvivalenssiluokkien joukko. Joukon $\mathbb{Z}$ alkioita kutsutaan kokonaisluvuiksi. Esimerkiksi $[(3,1)] = \{(3,1),(4,2),\ldots\}$. Kirjoitamme $0 = [(1,1)]$ ja $1 = [(2,1)]$. Näin ollen nyt on käytössä kaksi merkitystä merkinnälle "1". Tätä seikkaa tarkastellaan ja merkitykset sovitetaan yhteen myöhemmin.

On huomattava, että 0 ja 1 ovat erillisiä kokonaislukuja, $(1,1) \in 0$ mutta $(1,1) \notin 1$, koska $1+1 = 2$ ja $2+1 = 3 \neq 2$. Lisäksi pätee $(m,n) \in 0$ jos ja vain jos $(m,n) \sim (1,1)$. Lauseen 2.2.5 mukaan $(m,n) \in 0$ jos ja vain jos $m = n$, koska $(m,n) \sim (1,1)$ jos ja vain jos $m+1 = n+1$.

Ennen kuin esittelemme idean kokonaislukujen yhteenlaskusta todistamme lemman joka takaa, että yhteenlaskun käsite on hyvin määritelty.

Lemma 3.1.4. *Olkoon* g,h,i,j,k,l,m,n *luonnollisia lukuja. Jos* $(g,h) \sim (k,l)$ *ja* $(i,j) \sim (m,n)$, *niin*

$$(g+i, h+j) \sim (k+m, l+n).$$

Todistus. Alkutietona on, että $g+l = h+k$ ja $i+n = j+m$. Tällöin

$$\begin{aligned} g+i+l+n &= g+l+i+n \\ &= h+k+j+m \\ &= h+j+k+m, \end{aligned}$$

kuten vaadittiinkin. □

Jos $k > l$ ja $m > n$, niin

$$k + m = l + (k - l) + n + (m - n),$$

ja edelleen

$$(k - l) + (m - n) = (k + m) - (l + n).$$

3.2 Kokonaislukujen ominaisuuksia

Olkoon $a = [(k, l)]$ ja $b = [(m, n)]$, jossa k, l, m, n ovat luonnollisia lukuja. Määritämme

$$a + b = [(k + m, l + n)].$$

Esimerkiksi $0 + 1 = [(1, 1)] + [(2, 1)] = [(3, 2)] = [(2, 1)] = 1$. Lemman 3.1.4 mukaan jos $(g + i, h + j) \sim (k + m, l + n)$, niin g, h, i, j ovat luonnollisia lukuja siten, että $(g, h) \sim (k, l)$ ja $(i, j) \sim (m, n)$.

Näin ollen $(g + i, h + j)$ ja $(k + m, l + n)$ määräävät saman ekvivalenssiluokan $a + b$. Kääntäen luokan $a + b$ määritelmässä ei ole väliä mitkä (k, l) ja (m, n) valitaan ekvivalenssiluokista a ja b. Toisin sanoen, $a + b$ on yksikäsitteinen ekvivalenssiluokka ja näin ollen $a + b$ on hyvin määritelty. Lukua $a + b$ kutsutaan lukujen a ja b *summaksi* ja binäärioperaatiota jota merkitään $+$ joukossa $\mathbb{Z}$ *yhteenlaskuksi*.

Etenemme tarkastelemaan yhteenlaskun ominaisuuksia kokonaislukujen joukossa $\mathbb{Z}$. Seuraavat kaksi lausetta, kokonaislukujen yhteenlaskun vaihdannaisuus ja liitännäisyys, saadaan helposti vastaavista luonnollisten lukujen ominaisuuksista.

Lause 3.2.1. *Kaikilla $a \in \mathbb{Z}$ ja $b \in \mathbb{Z}$ pätee $a + b = b + a$.*

Todistus. Valitaan $(k, l) \in a$ ja $(m, n) \in b$. Tällöin

$$a + b = [(k + m, l + n)] = [(m + k, n + l)] = b + a.$$

□

Lause 3.2.2. *Jos $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, niin $a + (b + c) = (a + b) + c$.*

Todistus. Valitaan $(i, j) \in a, (k, l) \in b$ ja $(m, n) \in c$. Tällöin

$$\begin{aligned} a + (b + c) &= [(i, j)] + ([(k, l)] + [(m, n)]) \\ &= [(i, j)] + [(k + m, l + n)] \\ &= [(i + (k + m), j + (l + n))] \\ &= [((i + k) + m, (j + l) + n)] \\ &= [(i + k, j + l)] + [(m, n)] \\ &= ([(i, j)] + [(k, l)]) + [(m, n)] \\ &= (a + b) + c. \end{aligned}$$

□

Seuraava lause toteaa, että 0 on yhteenlaskun *neutraalialkio* kokonaislukujen joukossa.

Lause 3.2.3. *Kaikilla $a \in \mathbb{Z}$ pätee $a + 0 = a$.*

Todistus. Olkoon $(m, n) \in a$. Tällöin

$$a + 0 = [(m, n)] + [(1, 1)] = [(m + 1, n + 1)] = [(m, n)] = a.$$

□

Lause 3.2.4. *Jokaiselle $a \in \mathbb{Z}$ on olemassa $b \in \mathbb{Z}$ siten, että $a + b = 0$.*

Todistus. Valitaan $(m, n) \in a$ ja määritetään $b = [(n, m)]$. Tällöin

$$a + b = [(m, n)] + [(n, m)] = [(m + n, n + m)] = [(1, 1)] = 0.$$

□

Tämä tarkoittaa, että jokaiselle kokonaisluvulle on olemassa *vastaluku*.

Lemma 3.2.5. *Olkoon g, h, i, j, k, l, m, n luonnollisia lukuja. Jos $(g, h) \sim (k, l)$ ja $(i, j) \sim (m, n)$, niin*

$$(gi + hj, hi + gj) \sim (km + ln, lm + kn).$$

Todistus. Osoitetaan ensin, että $(gi + hj, hi + gj)$ ja $(km + ln, lm + kn)$ ovat ekvivalentteja alkion $(ki + lj, li + kj)$ kanssa, jolloin ekvivalenssirelaation transitiivisuus täydentää todistuksen.

Nyt $g + l = h + k$, koska $(g, h) \sim (k, l)$ Tästä johtuen

$$\begin{aligned} gi + hj + li + kj &= gi + li + hj + kj \\ &= i(g + l) + j(h + k) \\ &= i(h + k) + j(g + l) \\ &= ih + ik + jg + jl \\ &= hi + gj + ki + lj \end{aligned}$$

ja niin

$$(gi + hj, hi + gj) \sim (ki + lj, li + kj).$$

Koska $(m, n) \sim (i, j)$, saadaan vastaavalla perustelulla

$$(km + ln, lm + kn) \sim (ki + lj, li + kj),$$

ja tästä seuraa lemman tulos. □

Jos $k > k$ ja $m > n$, niin

$$\begin{aligned} km + ln &= (l + (k - l))m + ln \\ &= lm + (k - l)(n + (m - n)) + ln \\ &= lm + ln + (k - l)n + (k - l)(m - n) \\ &= lm + n(l + (k - l)) + (k - l)(m - n) \\ &= lm + kn + (k - l)(m - n). \end{aligned}$$

Siten

$$(k - l)(m - n) = (km + ln) - (lm + kn).$$

Olkoon $a = [(k, l)]$ ja $b = [(m, n)]$, jossa k, l, m, n ovat luonnollisia lukuja. Määrittelemme

$$ab = [(km + ln, lm + kn)].$$

Lemma 3.2.5 takaa, että ab on hyvin määritelty: Ei ole merkitystä mitkä järjestetyt parit $(k, l) \in a$ ja $(m, n) \in b$ valitaan luvun ab määritelmässä.

Lukua ab kutsutaan lukujen a ja b *tuloksi*, ja juuri määritelty laskutoimitus on nimeltään *kertolasku*. Merkinnän ab sijaan voidaan kirjoittaa $a \cdot b$.

Kokonaislukujen kertolaskulle pätee vaihdannaisuus.

Lause 3.2.6. *Kaikilla $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ pätee $ab = ba$.*

Todistus. Valitaan $(k,l) \in a$ ja $(m,n) \in b$. Tällöin

$$ab = [(km + ln, lm + kn)] = [(mk + nl, nk + ml)] = ba.$$

□

Seuraava lause osoittaa, että kokonaislukujen kertolasku on liitännäinen.

Lause 3.2.7. *Jos* $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, *niin* $a(bc) = (ab)c$.

Todistus. Valitaan $(i,j) \in a, (k,l) \in b$ ja $(m,n) \in c$. Tällöin

$$bc = [(km + ln, lm + kn)],$$

ja siten

$$\begin{aligned} a(bc) &= [(i(km + ln) + j(lm + kn), j(km + ln) + i(lm + kn))] \\ &= [(ikm + iln + jlm + jkn, jkm + jln + ilm + ikn)]. \end{aligned}$$

Vastaavasti

$$\begin{aligned} (ab)c &= c(ab) \\ &= [(mik + mjl + njk + nil, nik + njl + mjk + mil)] \\ &= [(ikm + iln + jlm + jkn, jkm + jln + ilm + ikn)] \\ &= a(bc). \end{aligned}$$

□

Lause 3.2.8. *Jos* $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, *niin* $a(b + c) = ab + ac$.

Todistus. Luonnollisten lukujen ominaisuuksien nojalla saadaan

$$\begin{aligned} a(b + c) &= [(i,j)][(k + m, l + n)] \\ &= [(i(k + m) + j(l + n), j(k + m) + i(l + n))] \\ &= [(ik + im + jl + jn, jk + jm + il + in)] \end{aligned}$$

ja

$$\begin{aligned} ab + ac &= [(ik + jl, jk + il)] + [(im + jn, jm + in)] \\ &= [(ik + jl + im + jn, jk + il + jm + in)] \\ &= [(ik + im + jl + jn, jk + jm + il + in)] \\ &= a(b + c). \end{aligned}$$

□

On huomioitava, että jos $(m, n) \in \mathbb{N} \times \mathbb{N}$, niin

$$\begin{aligned}[(m+1,1)] + [(n+1,1)] &= [(m+n+2,2)] \\ &= [(m+n+1,1)]\end{aligned}$$

ja

$$\begin{aligned}[(m+1,1)][(n+1,1)] &= [((m+1)(n+1)+1, n+1+m+1) \\ &= [(m(n+1)+n+1+1, n+m+2)] \\ &= [(mn+m+n+2, m+n+2)] \\ &= [(mn+1,1)].\end{aligned}$$

Tästä johtuen näemme, että $[(n+1,1)]$ toteuttaa vastaavat säännöt kuin jotka ovat voimassa luvulle n luonnollisten lukujen joukossa $\mathbb{N}$. Määritellään

$$\Phi(n) = [(n+1,1)]$$

kaikilla $n \in \mathbb{N}$. Tällöin edellä olevat laskutoimitukset osoittavat, että

$$\Phi(m) + \Phi(n) = \Phi(m+n)$$

ja

$$\Phi(m)\Phi(n) = \Phi(mn).$$

Nähdään myös, että Φ on injektio joukosta $\mathbb{N}$ joukkoon $\mathbb{Z}$. Oletetaan, että $\Phi(m) = \Phi(n)$. Tällöin $[(m+1,1)] = [(n+1,1)]$, joten $(m+1,1) \sim (n+1,1)$. Toisin sanoen $m+2 = n+2$. ja siten $m = n$.

Siis funktio Φ asettaa yksi-yhteen vastaavuuden joukon $\mathbb{N}$ ja joukon $\mathbb{Z}$ osajoukon välille. Lisäksi, alkion $m+n$ kuva tämän vastaavuuden valossa on alkioiden m ja n kuvien summa. Sama väittämä pätee myös tuloille.

Tämä tarkoittaa karkeasti ilmaistuna, että kokonaislukuja jotka ovat muotoa $[(n+1,1)]$, jossa $n \in \mathbb{N}$, voidaan käsitellä kuten ne olisivat luonnollisia lukuja.

Kerrataan muutaman algebrallisen rakenteen määritelmä, jotta voimme yleistää saamamme tulokset jatkoa varten. Nämä määritelmät on esitetty lähdeteoksissa [1], [5] ja [6].

Määritelmä 3.2.9. *Abelin ryhmä* on pari $(R, +)$, jossa joukon alkioille $a, b, c \in R$ pätee:

(a) Alkio $a+b$ on joukon yksikäsitteinen alkio eli R on binäärioperaation $+$ suhteen suljettu ;

(b) Vaihdannaisuus : $a+b=b+a$;

(c) Liitännäisyys : $(a+b)+c=a+(b+c)$;

(d) Neutraalialkio : On olemassa alkio i jolle $a+i=i+a=a$;

(e) Käänteisalkio : Kaikilla a on olemassa alkio $-a$, jolle pätee $a+(-a)=i$.

Mikäli ehdot (a),(c)-(e) ovat voimassa, kyseessä on *ryhmä*. *Puoliryhmässä* ei ole käänteisalkiota eikä neutraalialkiota : Näin ollen puoliryhmän ehdoiksi riittävät edellä olevista Abelin ryhmän ehdoista (a) ja (c) eli puoliryhmä on laskutoimituksen suhteen suljettu ja liitännäisyys on voimassa.

Määritelmä 3.2.10. Kolmikko $(R,+,\cdot)$ on *rengas*, kun sillä on seuraavat ominaisuudet:

(a) $(R,+)$ on Abelin ryhmä (neutraalialkio 0) ;

(b) Laskutoimitus $\cdot$ on liitännäinen joukossa R ;

(c) Osittelulait pätevät eli

$$a\cdot(b+c)=ab+ac$$
$$(a+b)\cdot c=ac+bc,$$

kun $a,b,c\in R$.

Määritelmä 3.2.11. *Kokonaisalue* on vaihdannainen ja ykkösellinen rengas, joka ei sisällä nollantekijöitä.

Renkaassa R *nollantekijä* on nollasta poikkeava alkio $r\in R\setminus\{0\}$ jolle on olemassa $s\in R\setminus\{0\}$ niin, että $rs=0$.

Määritelmä 3.2.12. Olkoon $(R,+,\cdot,0,1)$ kokonaisalue. Oletetaan, että $<$ on relaatio joukossa R ja toteuttaa seuraavat ehdot kaikilla $(a,b,c)\in R\times R\times R$:

(a) $a\not<a$;

(b) Jos $a<b$ ja $b<c$, niin $a<c$;

(c) $a=b, a<b$ tai $a>b$;

(d) Jos $a < b$, niin $a + c < b + c$;

(e) Jos $a < b$ ja $c > 0$, niin $ac < bc$.

Tällöin $(R, +, \cdot, 0, 1, <)$ on *järjestetty kokonaisalue.*

Tarkastellaan vielä potenssilaskua kokonaisalueessa. Määritellään ensin lyhentääksemme ilmaisuja uusi merkintätapa, jota kutsutaan tulo-operaattoriksi.

Olkoon $G : \mathbb{N} \to X$ funktio. Näin G kuvaa jokaisen luonnolliset luvun jollekin joukon X alkiolle. Olkoon $F : \mathbb{N} \times X \to \mathbb{N} \times X$ kuvaus niin, että $F(n, x) = (n + 1, x \cdot G(n + 1))$ kaikilla $(n, x) \in \mathbb{N} \times X$. Rekursiolauseen mukaan, jokaisella luvulla $m \in \mathbb{N}$ on olemassa yksikäsitteinen funktio $H_m : \mathbb{N} \to \mathbb{N} \times X$ niin, että $H_m(1)$ on alkio $(m, G(m))$ joukossa $\mathbb{N} \times X$ ja lisäksi pätee $H_m \circ S = F \circ H_m$. Näin ollen

$$H_m(n + 1) = F(H_m(n))$$

kaikilla $n \in \mathbb{N}$. Esimerkiksi

$$\begin{aligned} &H_m(1) = (m, G(m)), \\ &H_m(2) = F(H_m(1)) = F(m, G(m)) = (m + 1, G(m) \cdot G(m + 1)) \end{aligned}$$

ja

$$\begin{aligned} H_m(3) = F(H_m(2)) &= F(m + 1, G(m) \cdot G(m + 1)) \\ &= (m + 2, G(m) \cdot G(m + 1) \cdot G(m + 2)). \end{aligned}$$

Seuraavaksi, määritellään $P(n, n) = G(n)$ jokaisella $n \in \mathbb{N}$. Jokaiselle luonnolliselle luvulle $m < n$ määritellään $P(m, n)$ olemaan jälkimmäinen luku lukuparista $H_m(l + 1)$ ja l on yksikäsitteinen luonnollinen luku niin, että $m + l = n$. Esimerkiksi

$$\begin{aligned} &P(1, 3) = G(1) \cdot G(2) \cdot G(3); \\ &P(2, 3) = G(2) \cdot G(3); \\ &P(3, 3) = G(3). \end{aligned}$$

Lemma 3.2.13. *Jokaisella $(m, n) \in \mathbb{N} \times \mathbb{N}$, jossa $m \leq n$ pätee*

$$P(m, n + 1) = P(m, n) \cdot G(n + 1).$$

Todistus. Jos $m = n$, niin $m+l = n+1$ kun $l = 1$ ja $P(m, n+1)$ on lukuparin $H_m(2)$ jälkimmäinen luku

$$G(m) \cdot G(m + 1) = G(n) \cdot G(n + 1) = P(n, n) \cdot G(n + 1)$$

kuten pitikin.

Toisaalta oletetaan, että $m < n$. Tällöin $m + l = n$ jollakin luonnollisella luvulla n ja niin $m+l+1 = n+1$ sekä $P(n, n+1)$ on jälkimmäinen lukuparin $H_m(l+2)$ luvuista.

Osoitamme induktiolla luvun l suhteen, että ensimmäinen lukuparin $H_m(l+1)$ luvuista on $m + l = n$. Itseasiassa ensimmäinen lukuparin $H_m(2)$ luvuista on $m+1$ ja jos $H_m(l+1) = (m+l, P(m, n))$ jollakin $n \in l$, tällöin ensimmäinen osatekijä $H_m(l+2) = F(H_m(l+1)) = F(m+l, P(m, n))$ on $m + l + 1$ kuten pitikin. Koska toinen lukuparin $H_m(l+2) = F(n, P(m, n))$ luvuista on $P(m, n) + G(n+1)$ lemma pätee tässäkin tapauksessa. □

Määritämme nyt uuden merkintätavan edellä määritellylle luvulle $P(m, n)$.

$$P(m, n) = \prod_{k=m}^{n} G(k).$$

Voimme nyt määrittää potenssilaskun kokonaisalueessa edellisen määrittelyn erityistapauksena, valitsemalla $G(k) = a$. Olkoon $(R, +, \cdot, 0, 1)$ kokonaisalue. Tämä merkintä tarkoittaa, että joukossa R on yhteenlaskun neutraalialkiona luku 0 ja luku 1 kertolaskun neutraalialkio. Kaikilla luvuilla $a \in R$ pätee siis $a + 0 = a$ ja $a \cdot 1 = a$. Jokaisella $a \in R$ ja $n \in \mathbb{N}$ määrittelemme

$$a^n = \prod_{k=1}^{n} a.$$

Määrittelemme myös $a^0 = 1$ jos $a \neq 0$.

Jos $(a, n) \in \mathbb{N} \times \mathbb{N}$, niin yllä oleva merkintä täytyy sovittaa yhteen aiemmin käytetyn kanssa. Tämän yhteensovittaminen suoritetaan induktiolla. Ensiksi, $a^1 = \prod_{k=1}^{1} a = a$. Seuraavaksi oletetaan induktio-oletuksena, että $\prod_{k=1}^{n} a = a^n$ jollakin $n \in \mathbb{N}$ (jossa käytämme edeltävää määritelmää luvulle a^n). Tällöin

$$\prod_{k=1}^{n+1} a = a \prod_{k=1}^{n} a = a \cdot a^n = a^{n+1},$$

kuten vaadittiinkin. On huomattavaa yleisesti, että jos $(a, n) \in R \times \mathbb{N}$, niin

$$a^{n+1} = \prod_{k=1}^{n+1} a = a \prod_{k=1}^{n} a = a \cdot a^n.$$

Luku a^n on luvun a *kertaluvun* n *potenssi.* Jos $(a, b) \in R \times R$ on huomattava, että

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+ab+ba+b^2\\ &= a^2+2ab+b^2.\end{aligned}$$

Vastaavasti

$$\begin{aligned}(a-b)(a+b) &= a(a+b)+(-b)(a+b)\\ &= a^2+ab-ba-b^2\\ &= a^2-b^2.\end{aligned}$$

Lause 3.2.14. *Olkoon* $(R, +, \cdot, 0, 1)$ *kokonaisalue. Olkoon* $(a, b) \in R \times R$ *ja olkoon* $n \in \mathbb{N}$*. Tällöin*

$$(ab)^n = a^n b^n.$$

Todistus. Molemmat ovat yhtäsuuria kuin ab jos $n = 1$. Oletaan induktio-oletuksena, että $(ab)^n = a^n b^n$ jollakin $n \in \mathbb{N}$. Tällöin

$$(ab)^{n+1} = ab(ab)^n = aba^n b^n = (a \cdot a^n)(b \cdot b^n) = a^{n+1}b^{n+1}.$$

□

Lause 3.2.15. *Olkoon* $(R, +, \cdot, 0, 1)$ *kokonaisalue ja* $(a, m, n) \in R \times \mathbb{N} \times \mathbb{N}$*. Tällöin*

(a) $a^m a^n = a^{m+n}$

(b) $(a^m)^n = a^{mn}$.

Todistus. Lause on yleistys lauseista 2.2.14 sekä 2.2.15, jotka on jo todistettu aiemmin. Todistus seuraa kyseisten lauseiden todistusta, joten ohitamme sen tässä yhteydessä. □

Laajennamme seuraavaksi järjestysrelaation käsitteen, joka määriteltiin jo aiemmin luonnollisille luvuille, kokonaisluvuille.

Lemma 3.2.16. *Olkoon* $a \in \mathbb{Z}, (k, l) \in a$ *ja* $(m, n) \in a$*. Tällöin* $k < l$ *jos ja vain jos* $m < n$*.*

Todistus. Koska $(k,l) \in a$ ja $(m,n) \in a$, niin $(k,l) \sim (m,n)$ ja niin $k + n = l + m$. Oletetaan, että $k < l$. Jos $n \leq m$, päädytään ristiriitaan, että $k + n < l + m$. Näin ollen $m < n$. Vastaavasti jos $m < n$, niin $k < l$. □

Pätee myös, että $k > l$ jos ja vain jos $m > n$.

Olkoon $a \in \mathbb{Z}$ ja $(m,n) \in a$. Luvun a sanotaan olevan *positiivinen* jos $m > n$ ja *negatiivinen* jos $m < n$.

Edeltävä lemma varmistaa, että nämä käsitteet on hyvin määriteltyjä. Ei ole väliä mikä ekvivalenssiluokan a edustaja valitaan. On huomattava, että 0 ei ole negatiivinen eikä positiivinen, sillä $(1,1) \in 0$ ja $1 \not< 1$. Toisaalta 1 on positiivinen sillä $(2,1) \in 1$ ja $2 > 1$. Jokainen nollasta poikkeava kokonaisluku on joko negatiivinen tai posiitivinen.

Olkoon P positiivisten kokonaislukujen joukko. Valitaan $a \in P$ ja $(m,n) \in a$. Tällöin $m > n$ ja siten voimme kirjoittaa $m = n + k$ jollakin $k \in \mathbb{N}$. Siten $(n+k,n) \in a$ ja niin $(k+1,1) \in a$, koska $(n+k,n) \sim (k+1,1)$ määritelmän mukaan. Tästä johtuen $a \in \mathbb{N}$, aiemman kokonaislukujen muotoa $[(n+1,1)]$, $n \in \mathbb{N}$ määrittelyn mukaan.

Käänteisesti, jokainen luonnollinen luku on positiivinen, koska $n + 1 > 1$ kaikilla $n \in \mathbb{N}$. Voimme nyt samaistaa luonnolliset luvut positiivisiksi kokonaisluvuiksi. Tästä seuraa, että summat ja tulot positiivisille kokonaisluvuille ovat aina positiivisia.

Lemma 3.2.17. *Olkoon $a \in \mathbb{Z} \setminus \{0\}$. Tällöin joko a tai $-a$, mutta ei molemmat, on positiivinen.*

Todistus. Valitaan $(m,n) \in a$. Koska $a \neq 0$, pätee $m \neq m$. Jos $m > n$, niin a on positiivinen. Muutoin $m < n$. Tässä tapauksessa $-a$ on positiivinen, koska $-a = [(n,m)]$. Toisaalta a ja $-a$ eivät ole molemmat positiivisia, koska $a + (-a) = 0$, joka ei ole positiivinen. □

Jos $a = 0$, niin $-a = 0$. Näin ollen yksi edeltävän lemman seurauksista on, että $-a$ on positiivinen jos ja vain jos a on negatiivinen.

Olkoon $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. Kirjoitamme $a < b$ tai $b > a$ jos $b - a$ on positiivinen. Tässä tapauksessa sanotaan, että a on pienempi kuin b tai, että b on suurempi kuin a. Koska $b - a$ on positiivinen, on olemassa $n \in \mathbb{N}$ siten, että $b - a = n$. Tästä johtuen $a + n = b$ ja näin ollen jos a ja b ovat positiivisia, niin nykyiset merkintätavat ja terminologia on sovitettu yhteen aiemmin luonnollisille luvuille määriteltyjen kanssa.

Yllä olevista määritelmistä seuraa välittömästi, että kokonaisluku $a = a - 0$ on positiivinen, jos ja vain jos $a > 0$. Vastaavasti a on negatiivinen jos ja vain jos $a < 0$. Jos $a \neq 0$, niin sanotaan, että luvun a *etumerkki* on positiivinen tai negatiivinen, riippuen onko $a > 0$ vai $a < 0$.

Symboli "<"määrittelee relaation joukossa $\mathbb{Z}$. Jos $a \in \mathbb{Z}$, niin $a \not< a$, sillä $a-a=0$, joka ei ole positiivinen. Relaatio $<$ ei tästä syystä ole refleksiivinen. Se on kuitenkin transitiivinen. Oletetaan $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, $a<b$ ja $b<c$. Tällöin $b-a>0$ ja $c-b>0$. Siis $c-a=c-b+b-a>0$, ja siten $a<c$.

Palautetaan mieleen, että jos $(a,b) \in \mathbb{Z}\times\mathbb{Z}$ ja $b-a \neq 0$, niin joko $b-a$ tai $-(b-a)$ on positiivinen. Jos $b-a>0$, niin $a<b$ määritelmän mukaan. Toisaalta jos $-(b-a)=a-b>0$, niin $a>b$. Toki jos $b-a=0$, niin $a=b$. Täten yhden vaihtoehdoista $a=b$, $a<b$ tai $a>b$ on pädettävä.

Seuraava lause osoittaa, että epäyhtälön molemmille puolille voidaan lisätä sama kokonaisluku.

Lause 3.2.18. *Olkoon $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. Jos $a<b$, niin $a+c<b+c$.*

Todistus. Koska $a<b$, niin $b-a$ on positiivinen. Tästä johtuen

$$b+c-(a+c)=b+c-a-c=b-a>0$$

ja siten $a+c<b+c$. □

Lemma 3.2.19. *Olkoon $(a,b) \in \mathbb{Z}\times\mathbb{Z}$. Jos $a<b$, niin $a+1 \leq b$.*

Todistus. Muutoin $a<b<a+1$. Vähentämällä a, saadaan $0<b-a<1$. Koska $b-a>0$, on $b-a \in \mathbb{N}$. Ei ole olemassa luonnollista lukua joka on pienempi kuin 1. Tästä ristiriidasta seuraa $a+1 \leq b$. □

Lause 3.2.20. *Olkoon $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. Jos $a<b$ ja $c>0$, niin $ac<bc$.*

Todistus. Koska $a<b$, saadaan $b-a>0$. Siten

$$bc-ac=c(b-a)>0,$$

koska $c>0$. Tämä päättely perustuu siihen, että positiiviset kokonaisluvut voidaan samaistaa luonnollisiksi luvuiksi ja näin ollen positiivisten kokonaislukujen tulo on myös positiivinen kokonaisluku. Näin ollen saadaan $bc>ac$ eli $ac<bc$. □

Lause 3.2.20 tarkoittaa siis sitä, että epäyhtälön molemmat puolet voidaan kertoa positiivisella kokonaisluvulla.

Olkoon $(R,+,\cdot,0,1,<)$ järjestetty kokonaisalue. Jos $(a,b) \in R\times R$ ja $b^2=a$, alkiota b kutsutaan luvun a *neliöjuureksi*. Tällöin merkitään $\sqrt{a}=b$. Alkion a *itseisarvo* joukossa R merkitään $|a|$ ja se määritellään neliöjuuren avulla, $|a|=\sqrt{a^2}$.

Lause 3.2.21. *Olkoon $(R,+,\cdot,0,1,<)$ järjestetty kokonaisalue ja $(a,b) \in R\times R$ jossa $b>0$. Tällöin $|a|<b$ jos ja vain jos $-b<a<b$.*

Todistus. Oletetaan, että $|a| < b$. Tällöin itseisarvon määritelmän nojalla $\sqrt{a^2} < b$. Korottamalla toiseen potenssiin, saamme $a^2 < b^2$ ja siten

$$0 > a^2 - b^2 = (a - b)(a + b).$$

Siis toinen luvuista $a - b$ ja $a + b$ on negatiivinen ja toinen positiivinen. Koska $b > 0 > -b$, saadaan $a - b < a + b$ ja niin $a - b < 0$ ja $a + b > 0$. Siis $-b < a < b$. Tämä perustelu voidaan kääntää, jos $-b < a < b$, niin $|a| < b$. □

Seuraavaa tulosta kutsutaan *kolmioepäyhtälöksi.*

Lause 3.2.22. *Jos* $(R, +, \cdot, 0, 1, <)$ *on järjestetty kokonaisalue ja* $(a, b) \in R \times R$, *niin* $|a + b| \leq |a| + |b|$.

Todistus. Pätee siis $-|a| \leq a \leq |a|$ ja $-|b| \leq b \leq |b|$. Yhteenlaskusta saadaan

$$-(|a| + |b|) \leq a + b \leq |a| + |b|,$$

ja siten Lauseen 3.2.21 nojalla $|a + b| \leq |a| + |b|$. □

Kolmioepäyhtälön merkitys geometrian näkökulmasta on se, että kolmion sivun pituus on vähintään kolmion kahden muun sivun pituuksien erotuksen itseisarvo ja korkeintaan yhtä suuri kuin kahden muun sivun pituuksien summa.

4 Rationaaliluvut

Jakolaskua, eli käänteistä kertolaskua, ei voida suorittaa rajoituksetta kokonaislukujen joukossa. Murtolukuja, jotka tekevät jakolaskun aina mahdolliseksi, pohdittiin jo varhaisina aikoina. Niitä ei koskaan pidetty mysteerinä, kuten edellä kerrottiin negatiivisista luvuista.

Edellisessä luvussa laajensimme luonnollisten lukujen joukon sisältämään myös negatiiviset kokonaisluvut ja näin muodostettiin järjestelmä joka on suljettu vähennyslaskun suhteen. Samalla tavalla kokonaislukujen järjestelmä voidaan laajentaa niin, että jos nolla poistetaan joukosta, on järjestelmä suljettu jakolaskun suhteen. Tätä laajennettua lukujärjestelmää kutsutaan rationaalilukujen järjestelmäksi. Rationaaliluvut tuovat monia etuja esimerkiksi fyysisten mittojen, kuten pituuksien, alojen ja tilavuuksien matemaattiseen käsittelyyyn.

Rationaaliluvut esitetään kokonaislukujen ekvivalenssiluokkina. Tämä seuraa Saksalaisen matemaatikon Heinrich Weberin esimerkkiä vuodelta 1895. Hänen teoksessaan "Lehrbuch der Algebra"rationaaliluvut on muodostettu samaisen mallin mukaisesti.

4.1 Rationaalilukujen määritelmä

Olkoon $(a, b) \in \mathbb{N} \times \mathbb{N}$, jossa $b > 1$. Tällöin $ab \geq b$, aina kun $a \geq 1$. Jos c on positiivinen ja lukua b pienempi kokonaisluku, niin ei olemassa kokonaislukua d siten, että $db = c$, sillä jos $d > 0$, niin $db \geq c$, jos $d = 0$ niin $db = 0 < c$ ja jos $d < 0$, niin $db < 0 < c$. Tämä tarkastelu perustelee taas yhden uudenlaisen luvun kehityksen.

Kuten kokonaislukujen tapauksessa, aloitamme määrittelemällä ekvivalenssirelaation. Tällä kertaa ekvivalenssirelaatio tosin on joukossa $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Olkoon a, b, c, d kokonaislukuja siten, että $b \neq 0$ ja $d \neq 0$. Tässä luvussa määrittelemme $(a, b) \sim (c, d)$ tarkoittamaan, että $ad = bc$. Esimerkiksi $(1, 2) \sim (2, 4)$, koska $1 \cdot 4 = 2 \cdot 2 = 4$. On huomattava, että $(a, b) \sim (ac, bc)$ jos $c \neq 0$ ja $b \neq 0$. Esimerkiksi $(c, c) \sim (1, 1)$.

Lause 4.1.1. *Relaatio $\sim$ on ekvivalenssirelaatio joukossa $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

Todistus. Kertolaskun kommutatiivisuudesta seuraa suoraan, että $(a, b) \sim (a, b)$ kaikilla $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Täten refleksiivisyys pätee. Symmetria seuraa suoraan yhtäsuuruuden symmetriasta ja kertolaskun kommutatiivisuudesta.

Oletetaan, että $(a, b) \sim (c, d)$ ja $(c, d) \sim (e, f)$. Täten a, b, c, d, e, f ovat kokonaislukuja siten, että $b \neq 0, d \neq 0, f \neq 0, ad = bc$ ja $cf = de$. Näin ollen $adf = bcf = bde$ ja koska $d \neq 0$, seuraa, että $af = be$. Toisin sanoen $(a, b) \sim (e, f)$ eli transitiivisuus on voimassa ja $\sim$ on siten ekvivalenssirelaatio. □

Olkoon $\mathbb{Q}$ relaation $\sim$ ekvivalenssiluokkien joukko. Joukon $\mathbb{Q}$ alkiot ovat *rationaalilukuja*. Esimerkiksi $[(1, 2)] = \{(1, 2), (2, 4), \ldots\}$. Merkitään $0 = [(0, 1)]$ ja $1 = [(1, 1)]$. Nämä uudet symbolien "0"ja "1"käyttökohteet sovitetaan aiempien kanssa myöhemmin. On huomattavaa, että $(a, b) \in 0$ jos ja vain jos $a = 0$, tälle on edellytys $(a, b) \sim (0, 1)$. Vastaavasti $(a, b) \in 1$ jos ja vain jos $a = b$. Esimerkiksi $(1, 1) \notin 0$ mutta $(1, 1) \in 1$ ja siten voimme päätellä, että $0 \neq 1$.

Rationaaliluku $[(a, b)]$ kirjoitetaan normaalisti $\frac{a}{b}$ tai a/b. Täten $0 = 0/1$ ja $1 = 1/1$. Lisäksi jos $bc \neq 0$, niin

$$\frac{ac}{bc} = \frac{a}{b}.$$

Esimerkiksi $1/2 = 2/4 = (-2)/(-4)$. On myös huomattava, että $a/a = 1/1 = 1$ jos $a \neq 0$.

4.2 Rationaalilukujen ominaisuuksia

Kuten kokonaislukujen tapauksessa, yhteen- ja kertolaskun määritelmät vaativat ennakoivat lemmat perusteluikseen.

Lemma 4.2.1. *Olkoon a, b, c, d, e, f, g, h kokonaislukuja siten, että $bdfh \neq 0$. Jos $(a, b) \sim (e, f)$ ja $(c, d) \sim (g, h)$, niin*

$$(ad + bc, bd) \sim (eh + fg, fh).$$

Todistus. Huomataan ensin, että $bd \neq 0$ ja $fh \neq 0$. Saadaan $af = be$ ja $ch = dg$. Tästä johtuen

$$\begin{aligned} fh(ad + bc) &= adfh + bcfh = bdeh + bdfg \\ &= bdeh + bdfg = bd(eh + fg). \end{aligned}$$

□

Olkoon $q = [(a, b)]$ ja $r = [(c, d)]$, jossa a, b, c, d ovat kokonaislukuja ja $bd \neq 0$. Määrittelemme

$$q + r = [(ad + bc, bd)].$$

Edeltävän lemman mukaan, jos e, f, g, h ovat kokonaislukuja siten, että $fh \neq 0, (a, b) \sim (e, f)$ ja $(c, d) \sim (g, h)$, niin tällöin

$$(ad + bc, bd) \sim (eh + fg, fh).$$

Näin ollen $(ad + bc, bd)$ ja $(eh + fg, fh)$ määrittävät saman ekvivalenssiluokan $q + r$. Toisin sanoen $q + r$ on hyvin määritelty. Kutsutaan $q + r$ lukujen q ja r *summaksi* ja binäärioperaatiota jota merkitään $+$ *yhteenlaskuksi* joukossa $\mathbb{Q}$.

On huomattavaa, että

$$q + r = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Lemma 4.2.2. *Olkoon a, b, c, d, e, f, g, h kokonaislukuja siten, että $bdfh \neq 0$. Jos $(a, b) \sim (e, f)$ ja $(c, d) \sim (g, h)$, niin*

$$(ac, bd) \sim (eg, fh).$$

Todistus. Jälleen $bd \neq 0, fh \neq 0, af = be$ ja $ch = dg$. Tästä johtuen $acfh = bdeg$ kuten oli osoitettava. □

Olkoon $q = [(a, b)]$ ja $r = [(c, d)]$, jossa a, b, c, d ovat kokonaislukuja siten, että $bd \neq 0$. Määrittelemme $q \cdot r = [(ac, bd)]$. Edeltävä Lemma 4.2.2 osoittaa, että $q \cdot r$ on hyvin määritelty. Kutsumme $q \cdot r$ lukujen q ja r *tuloksi* ja binäärioperaatiota jota merkitään $\cdot$ *kertolaskuksi* joukossa $\mathbb{Q}$. Normaalisti kirjoitamme qr sen sijaan, että kirjoittaisimme $q \cdot r$. On huomattava, että

$$qr = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Palautetaan mieleen vielä yksi algebrallinen rakenne, kunnan käsite.

Määritelmä 4.2.3. Olkoon kolmikko $(K, +, \cdot)$ rengas, ja $K_0 = K \setminus \{0\}$. Tällöin tämä rengas on *kunta*, jos $(K_0, \cdot)$ on Abelin ryhmä, eli seuraavat ehdot täyttyvät:

(a) $1 \neq 0$ eli kertolaskun neutraalialkion on oltava joukossa K_0 ;

(b) Jokaisella $a \neq 0$ on olemassa a^{-1}, jolla $a^{-1} \cdot a = 1$;

(c) $ab = ba$ kaikilla $a, b \in K$, eli kertolasku on vaihdannainen.

Laajennetaan potenssilaskun käsite rationaaliluvuille ja yleistetään se jatkoa varten koskemaan myös muita kuntia. Olkoon $(F, +, \cdot, 0, 1)$ kunta ja $q \in F \setminus \{0\}$. Mille tahansa ei-negatiiviselle kokonaisluvulle a, määritellään $q^a = \prod_{k=1}^{a} q$. Näin ollen $q^1 = q$, $q^0 = 1$ sekä $q^{-1} = 1/q$. Määritellään $q^{-a} = 1/q^a$. Täten $q^a q^{-a} = 1$, $q^a = 1/q^{-a}$ ja $q^{-a} = 1/q^a$. Viimeisestä yhtälöstä seuraa, että kun a on negatiivinen kokonaisluku, niin $q^a = 1/q^{-a}$. Tämä yhtälö pätee tästä johtuen millä tahansa luvulla a.

Lause 4.2.4. *Olkoon $(F, +, \cdot, 0, 1)$ kunta, $q \in F \setminus \{0\}, r \in F \setminus \{0\}$ ja $a \in \mathbb{Z}$. Tällöin*

$$(qr)^a = q^a r^a.$$

Todistus. Tämä tulos on todistettu kun $a \geq 0$ Lauseessa 2.2.13. Jos $a < 0$, niin $-a > 0$ ja

$$(qr)^a = \frac{1}{(qr)^{-a}} = \frac{1}{q^{-a} r^{-a}} = \frac{1}{q^{-a}} \cdot \frac{1}{r^{-a}} = q^a r^a.$$

□

Lause 4.2.5. *Olkoon $(F, +, \cdot, 0, 1)$ kunta, $q \in F \setminus \{0\}$ ja $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Tällöin*

$$q^a q^b = q^{a+b}.$$

Todistus. Tämä tulos on todistettu kun $a \geq 0$ ja $b \geq 0$ Lauseessa 2.2.14. Jos $a < 0, b < 0$, niin $-a > 0, -b > 0$ ja siten $a + b < 0$. Tässä tapauksessa

$$q^a q^b = \frac{1}{q^{-a}} \cdot \frac{1}{q^{-b}} = \frac{1}{q^{-a} q^{-b}} = \frac{1}{q^{-a-b}} = \frac{1}{q^{-(a+b)}}.$$

Voidaan olettaa yleispätevyyden kärsimättä, että $a \geq 0, b < 0$. Näin ollen $-b > 0$. Jos $a + b \geq 0$, niin $q^{a+b} q^{-b} = q^{a+b-b} = q^a$ ja toivottu tulos seuraa kertomalla molemmat puolet luvulla q^b. Jos $a + b < 0$, niin $q^{-(a+b)} q^a =$

$q^{-a-b+a} = q^{-b}$ ja kertomalla molemmat puolet luvulla $q^{a+b}q^b$ saadaan tulos $q^a q^b = q^{a+b}$. Näin ollen

$$\frac{q^a}{q^b} = q^a q^{-b} = q^{a-b}.$$

□

Lause 4.2.6. *Olkoon $(F, +, \cdot, 0, 1)$ kunta, $q \in F \setminus \{0\}$ ja $a \in \mathbb{Z} \times \mathbb{Z}$. Tällöin*

$$(q^a)^b = q^{ab}.$$

Todistus. Jos $b \geq 0$, niin voidaan käyttää induktiota muuttujan b suhteen. Tarkastellaan ensin, että molemmat puolet ovat yhtäsuuria kuin 1 jos $b = 0$. Oletetaan induktio-oletuksena, että $(q^a)^b = q^{ab}$ jollakin ei-negatiivisella kokonaisluvulla b. Tällöin

$$\begin{aligned}(q^a)^{b+1} &= (q^a)^b q^a = q^{ab} q^a \\ &= q^{ab+a} = q^{a(b+1)},\end{aligned}$$

kuten pitääkin.

Jos $b < 0$, niin $-b > 0$ ja siten

$$(q^a)^b = \frac{1}{(q^a)^{-b}} = \frac{1}{q^{-ab}} = q^{ab}.$$

□

Yleistämme nyt järjestyksen käsitteen, joka määriteltiin aiemmin kokonaislukujen tapauksessa. Aloitetaan lemmalla.

Lemma 4.2.7. *Olkoon a, b, c, d kokonaislukuja siten, että $bd \neq 0$ ja $(a, b) \sim (c, d)$. Tällöin $ab > 0$ jos ja vain jos $cd > 0$.*

Todistus. Oletetaan, että $ab > 0$. Koska $(a, b) \sim (c, d)$, pätee $ad = bc$. Näin ollen $abd^2 = b^2cd$. Koska $bd \neq 0$, pätee $b^2 > 0$ ja $d^2 > 0$. Koska $ab > 0$ teemme oletuksen perusteella johtopäätöksen, että $cd > 0$. Samalla tavalla jos $cd > 0$, niin $ab > 0$. □

Korvaamalla luvut a ja c luvuilla $-a$ ja $-c$, saamme $ab < 0$ jos ja vain jos $cd < 0$, sillä jos $(a, b) \sim (c, d)$, niin $(-a, b) \sim (-c, d)$.

Olkoon q rationaaliluku. Tällöin $q = a/b$ joillakin kokonaisluvuilla a ja b, $b \neq 0$. Jos $ab = 0$, niin $a = 0$, joten $q = 0$. Kääntäen, jos $q = 0$, niin $ab = 0$. Luku q on positiivinen jos $ab > 0$ ja negatiivinen jos $ab < 0$. Edeltävä lemma

takaa, että nämä käsitteet ovat hyvin määritelty. Kuten kokonaislukujen tapauksessa, luku 0 ei ole negatiivinen tai positiivinen, mutta jokainen nollasta poikkeava rationaaliluku on joko negatiivinen tai positiivinen.

Lisäksi q on negatiivinen jos ja vain jos $-q$ on positiivinen. Jos $q = a$ ja $b = 1$, q on positiivinen kun $a > 0$ ja negatiivinen kun $a < 0$. Täten määritelmämme positiivisista ja negatiivisista rationaaliluvuista täsmäävät aiempien määritelmien kanssa, jotka koskevat positiivisia ja negatiivisia kokonaislukuja.

Jokaisessa tapauksessa kirjoitamme $q > 0$ jos q on positiivinen ja $q < 0$ jos q on negatiivinen. Jos $q \neq 0$, niin tällöin sanomme, että luvun q etumerkki on positiivinen tai negatiivinen, riippuen onko $q > 0$ vai $q < 0$. Jos q ja r ovat rationaalilukuja, niin sanomme, että q on pienempi kuin r tai, että r on suurempi kuin q, jos $r - q > 0$. Tässä tapauksessa kirjoitamme $q < r$ tai $r > q$. Luku r on positiivinen jos ja vain jos r on suurempi kuin 0. Vastaavasti q on negatiivinen jos ja vain jos se on pienempi kuin 0. Tämä vastaa myös kokonaislukujen vastaavaa määritelmää joka esitettiin kokonaislukujen luvussa ja vastaavasti ilmaisemme $q \leq r$ tai $r \geq q$ jos joko $q < r$ tai $q = r$.

Olkoon q ja r positiivisia rationaalilukuja. Oletetaan, että $q = a/b$ ja $r = c/d$, missä a, b, c, d ovat kokonaislukuja ja $bd \neq 0$. Tällöin

$$q + r = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Nyt $ab > 0$ ja $cd > 0$, sillä $q > 0$ ja $r > 0$ ja siten

$$bd(ad + bc) = abd^2 + b^2cd > 0,$$

koska $b^2 > 0$ ja $d^2 > 0$, aina kun $b \neq 0$ ja $d \neq 0$. Tästä johtuen $q + r > 0$. Vastaavasti $qr = ac/bd > 0$ koska $abcd > 0$.

Teoria on saatu nyt samaan pisteeseen kuin kokonaislukujen tapauksessa ja voidaan osoittaa, että $(\mathbb{Q}, +, \cdot, 0, 1, <)$ on järjestetty kokonaisalue. Järjestettyä kokonaisaluetta $(F, +, \cdot, 0, 1, <)$ kutsutaan järjestetyksi kunnaksi jos $(F, +, \cdot, 0, 1)$ on kunta. Näin ollen $(\mathbb{Q}, +, \cdot, 0, 1, <)$ on järjestetty kunta. On huomattava, että järjestettyjen kuntien on toteutettava kaikki Määritelmän 3.2.12 eli järjestetyn kokonaisalueen määrittelyn asettamat ehdot.

Olkoon $(F, +, \cdot, 0, 1, <)$ järjestetty kunta ja valitaan $q \in F \setminus \{0\}$. Tällöin $qq^{-1} = 1 > 0$ ja siten $1/q \neq 0$ ja luvuilla q ja $1/q$ on sama etumerkki. Nyt oletetaan, että $0 < q < r$. Koska luvuilla r ja $1/r$ on oltava sama etumerkki, on $1/r > 0$. Vastaavasti $1/q > 0$ ja siten $1/qr > 0$. Kertomalla epäyhtälö $q < r$ luvulla $1/qr$ molemmin puolin saadaan $1/r < 1/q$.

Vastaavanlaisella perustelulla saadaan, että jos $q < r < 0$, niin $1/r < 1/q$. Toisaalta jos $q < 0 < r$, niin $1/q < 0 < 1/r$.

Valitaan nyt $q \in F$ ja $r \in F \setminus \{0\}$. Siis $q = qr/r$ ja siten

$$|q| = |\frac{q}{r}||r|.$$

Koska $r \neq 0$, on $|r| \neq 0$. Jakamalla luvulla $|r|$ saadaan tästä johtuen

$$|\frac{q}{r}| = \frac{|q|}{|r|}.$$

Lause 4.2.8. *Olkoon $(F, +, \cdot, 0, 1, <)$ järjestetty kunta ja olkoon q ja r joukon F alkioita siten, että $q < r$. Tällöin on olemassa $s \in F$ siten, että $q < s < r$.*

Todistus. Koska $q < r$, pätee $2q < r + q < 2r$. Jakamalla luvulla 2 (eli kertomalla luvulla $1/2$) saadaan

$$q < \frac{r+q}{2} < r,$$

ja siten haluttu tulos pätee luvulla $s = (r + q)/2$. □

Karkeasti ilmaistuna tämä tulos tarkoittaa, että kahden toisistaan eroavan järjestetyn kunnan alkion välissä on jokin näistä kahdesta eroava kolmas alkio. Se ei ole yksikäsitteinen. Esimerkiksi on $\frac{1}{2} > \frac{1}{3} > \frac{1}{5}$ ja $\frac{1}{2} > \frac{1}{4} > \frac{1}{5}$.

Tarkastellaan vielä muutamia rationaalilukujen ominaisuuksia, joita tulemme tarvitsemaan seuraavassa luvussa.

Lause 4.2.9. *Olkoon r ja s rationaalilukuja. Jos $r > 0$, niin on olemassa $N \in \mathbb{N}$ siten, että $s/n < r$ kaikilla $n > N$.*

Todistus. Jos $s \leq 0$, niin lause pätee valinnalla $N = 1$. Oletetaan, että $s > 0$. Koska r ja s ovat positiivisia rationaalilukuja, on olemassa positiiviset rationaaliluvut a, b, c, d siten, että $r = a/b$ ja $s = c/d$. Valitaan $N = c(b+1)$. Tällöin $1/n < 1/N$ kaikilla $n > N$ ja näin ollen

$$\frac{s}{n} < \frac{s}{N} = \frac{c}{dc(b+1)} = \frac{1}{d(b+1)},$$

kun $n > N$. Pätee siis $d \geq 1$, joten $1/d \leq 1$. Lisäksi $b + 1 > b$, joten $1/(b+1) < 1/b$. Näin ollen saadaan $s/n < 1/b$ kaikilla $n > N$ ja koska $a \geq 1$, pätee

$$\frac{s}{n} < \frac{1}{b} \leq \frac{a}{b} = r$$

kun $n > N$. □

Lause 4.2.10. *Olkoon r ja s rationaalilukuja, joille pätee $r < s$. Kaikilla positiivisilla rationaaliluvuilla p on olemassa $m-2$, jossa $m \in \mathbb{N}$, rationaalilukua $q_2, q_3, \ldots, q_{m-1}$, jossa $q_1 = r$ ja $q_m = s$, joille pätee*

$$0 < q_k - q_{k-1} < p$$

kaikilla $k \in \{2, 3 \ldots, m\}$.

Todistus. Valitaan mielivaltainen rationaaliluku p. Nyt $s-r \in \mathbb{Q}$ ja Lauseesta 4.2.9 seuraa, että on olemassa $N \in \mathbb{N}$ niin, että

$$\frac{s-r}{m} < p$$

kun $m > N$. Kaikilla kokonaisluvuilla $m > N+1$ saadaan

$$\frac{s-r}{m-1} < p.$$

Olkoon

$$q_k = q_{k-1} + \frac{s-r}{m-1}$$

kaikilla $k \in \{2, 3, \ldots, m-1\}$. Koska $q_1 = r$, saadaan induktioperiaatteen nojalla, että

$$q_k = r + \frac{(k-1)(s-r)}{m-1}$$

kaikilla $k \in \{1, 2, \ldots, m-1\}$. Siten

$$\begin{aligned} q_m - q_{m-1} &= s - r - \frac{(m-2)(s-r)}{m-1} \\ &= \frac{(m-1)(s-r) - (m-2)(s-r)}{m-1} \\ &= \frac{s-r}{m-1}. \end{aligned}$$

Todistus seuraa nyt siitä, että

$$q_k - q_{k-1} = \frac{s-r}{m-1}$$

kaikilla $k \in \{2, 3, \ldots, m\}$ ja

$$0 < \frac{s-r}{m-1} < p.$$

□

Lemma 4.2.11. *Olkoon r mielivaltainen positiivinen rationaaliluku. Tällöin on olemassa positiiviset rationaaliluvut a ja b joille pätee $a^2 < r < b^2$.*

Todistus. Jos $r < 1$, niin $r^2 < r < 1$ ja siten voidaan valita $a = r$ ja $b = 1$. Jos $r = 1$, niin $(1/2)^2 < 1 < 2^2$ ja siten voimme valita $a = 1/2$ ja $b = 2$. Jos $r > 1$, niin $1 < r < r^2$ ja voimme valita $a = 1$ ja $b = r$. □

Lause 4.2.12. *Olkoon r mielivaltainen positiivinen rationaaliluku ja n mielivaltainen luonnollinen luku. Tällöin on olemassa positiivinen rationaaliluku s jolle pätee*

$$r < s^2 < r + \frac{1}{n}.$$

Todistus. Valitaan mikä tahansa positiivinen rationaaliluku r ja luonnollinen luku n. Edeltävän Lemman 4.2.11 mukaan on olemassa positiiviset rationaaliluvut a ja b joille pätee $a^2 < r < b^2$. Siten $a < b$ ja Lause 4.2.10 osoittaa, että millä tahansa positiiviselle rationaaliluvulla p on olemassa rationaaliluvut $q_1, q_2, \ldots, q_m$, jossa $m \in \mathbb{N}$, siten, että

$$a = q_1 < q_2 < \ldots < q_{m-1} < q_m = b$$

ja

$$q_k - q_{k-1} < p$$

kaikilla $k \in \{2, 3, \ldots, m\}$. Koska $q_k < q_{k-1} + p$, pätee

$$q_k^2 < q_{k-1}^2 + 2q_{k-1}p + p^2$$

ja näin ollen

$$q_k^2 - q_{k-1}^2 < 2q_{k-1}p + p^2 = p(2q_{k-1} + p)$$

kaikilla $k \in 2, 3, \ldots, m$. Valitaan

$$p = \frac{1}{n(2b+1)}.$$

Nyt siis $q_{k-1} < q_m = b$ kaikilla $k \in \{2, 3, \ldots, m\}$ ja koska $b > 0$, pätee myös $0 < p < 1$. Tästä johtuen

$$q_k^2 - q_{k-1}^2 < p(2q_{k-1} + p) < p(2b + 1) = \frac{1}{n}$$

kaikilla $k \in \{2, 3, \ldots, m\}$.

Olkoon $M \subset \mathbb{N}$ joukko

$$\{k \in \{1, 2, \ldots, m\} : q_k^2 > r\}.$$

Joukko M on epätyhjä, sillä $q_m^2 = b^2 > r$. Täten Lauseen 2.2.21 nojalla joukolla M on pienin alkio j. On huomattava, että $j > 1$, koska $q_1^2 = a^2 < r$. Edelleen, $q_j^2 > r$ ja $q_{j-1}^2 \leq r$.

Nyt osoitamme, että voimme valita $s = q_j$. Riittää vahvistaa, että $q_j^2 < r + 1/n$. Oletetaan, että $q_j^2 \geq r + 1/n$. Koska $r \geq q_{j-1}^2$, saadaan

$$q_j^2 - q_{j-1}^2 \geq (r + \frac{1}{n}) - r = \frac{1}{n}.$$

Tämä epäyhtälö aiheuttaa ristiriidan. Tästä johtuen $q_j^2 < r + 1/n$, kuten oli osoitettava. □

5 Reaaliluvut

Vaikka rationaalilukujen järjestelmä on selkeästi käytännöllisempi verrattuna kokonaislukujen järjestelmään, on myös siinä puutteita. Esimerkiksi jos neliön pinta-ala on 3 neliömetriä, niin molempien sivujen pituus on $\sqrt{3}$. Toisaalta yhtälöllä $x^2 = 3$ ei ole ratkaisua rationaalilukujen joukossa. Rationaalilukujen järjestelmässä on myös muita puutteita, mutta nämä voidaan voittaa laajentamalla rationaaliluvuista uuteen joukkoon, reaalilukuihin.

Reaaliluvut, jotka sisältävät rationaaliluvut osajoukkona, voidaan esittää desimaalilukuina. Tässä tutkielmassa ohitamme desimaalilukujen tarkastelun. Desimaaliluvuista voi lukea lisää esimerkiksi lähdeteoksesta [1]. Reaaliluvut ovat erityisen tärkeitä geometrian sovelluksissa. Koska lukusuoran pisteiden joukon ja reaalilukujen joukon välille voidaan asettaa yksi-yhteen vastaavuus, minkä tahansa janan pituus voidaan esittää reaaliluvulla.

Irrationaaliluvut aiheuttivat huomattavaa päänvaivaa monille matemaatikoille aiemmin. Klassinen esimerkki irrationaaliluvusta keksittiin jo muinaisessa Kreikassa. Pythagoraan seuraajat tiesivät, Pythagoraan lauseen nojalla, että neliön sivun pituuden ollessa yksi, sen lävistäjän pituus on $\sqrt{2}$. Harmikseen he saivat huomata, että $\sqrt{2}$ ei ole rationaaliluku. Näin syntyi tarve rationaalilukujen joukon laajentamiselle ja reaalilukujen joukon muodostamiselle. Jo babylonialaiset työkentelivät rationaalisten likiarvojen kanssa edeten irrationaalisiin suhteisiin. Kreikkalaiset oppivat, että luku $\sqrt{2}$ on irrationaaliluku. Eukleides muodosti tälle myös todistuksen.

Saksalainen matemaatikko Georg Cantor tutki 1800-luvun loppupuolella irrationaalilukuja. Hänen perusideansa mukaan reaaliluvut voidaan esittää suppenevilla rationaalilukujen jonoilla. Kahdella rationaalijonolla on sama raja-arvo jos ja vain jos näiden erotusten jono suppenee kohti nollaa. Tästä johtuen on luonnollista määrittää reaaliluvut suppenevien rationaalijonojen luokkina. Kaksi jonoa on ekvivalentteja kun niiden erotusten jono suppenee nollaan. Jotta tämä määritelmä olisi mielekäs, on jonon suppeneminen määritettävä käyttämättä sen raja-arvoa. Tämä voidaan toteuttaa käyttäen Cauchyn suppenemisehtoa. Seuraavaksi muodostamme reaalilukujen joukon Cantorin esimerkkiä seuraten.

5.1 Reaalilukujen määritelmä ja ominaisuuksia

Reaalilukujen määrittelemiseksi, määrittelemme ja tarkastelemme ensin muutamia jonoihin liittyviä käsitteitä.

Määritelmä 5.1.1. *Jono* joukossa X on kuvaus $f : \mathbb{N} \to X$. Jonon arvojoukon alkioita kutsutaan *termeiksi*.

Jono voidaan esittää monella tapaa. Täsmällisesti ilmaistuna jono $f : \mathbb{N} \to X$ esitetään järjestettyjen parien joukkona

$$\{(1, f(1)), (2, f(2)), \ldots\}.$$

Yleensä jono esitetään muodossa $(a_n) = a_1, a_2, a_3, \ldots$.

Määritelmä 5.1.2. Rationaalilukujen jono (a_n) on rationaalisesti *suppeneva*, jos on olemassa sellainen rationaaliluku a, että jokaiselle $\epsilon > 0$ on olemassa jokin luku $k \in \mathbb{N}$, jolle pätee $|a_n - a| < \epsilon$ kaikilla $n \geq k$. Tällöin a on määritelty yksikäsitteisesti ja voidaan kirjoittaa $a = \lim_{n\to\infty} a_n$

Määritelmä 5.1.3. Jono (a_n) on *Cauchyn jono*, jos jokaisella positiivisella rationaaliluvulla ϵ on olemassa jokin $N \in \mathbb{N}$ siten, että $|a_n - a_m| < \epsilon$, kun $n > N$ ja $m > N$.

Ehdon mukaan jonon jäsenet kasautuvat mielivaltaisen lähelle toisiaan jonon edetessä. On huomattava, että jos (a_n) on Cauchyn jono niin tällöin myös $(-a_n)$ on Cauchyn jono.

Lause 5.1.4. *Jokainen suppeneva jono joukossa $\mathbb{Q}$ on Cauchyn jono.*

Todistus. Olkoon (a_n) joukon $\mathbb{Q}$ suppeneva jono, $\lim_{n\to\infty} a_n = a$. Valitaan $\epsilon > 0$. Täytyy osoittaa, että on olemassa N siten, että $|a_n - a_m| < \epsilon$ kun

$n > N$ ja $m > N$. Koska $a_n \to a$, on olemassa N siten, että $|a_n - a| < \epsilon/2$ kaikilla $n > N$. Olkoon $n > N$ ja $m > N$, tällöin

$$\begin{aligned} |a_n - a_m| &= |a_n - a + a - a_m| \\ &\leq |a_n - a| + |a_m - a| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \end{aligned}$$

ja näin ollen (a_n) on Cauchyn jono. □

Lemma 5.1.5. *On olemassa positiivisten rationaalilukujen jono (a_n), jolle pätee $a_n^2 \to 2$, kun $n \to \infty$.*

Todistus. Valitaan $\epsilon > 0$. Lauseesta 4.2.12 seuraa, että millä tahansa $n \in \mathbb{N}$ on olemassa positiivinen luku a_n jolle pätee $2 < a_n^2 < 2 + 1/n$. Olkoon (a_n) sellainen jono joukossa $\mathbb{Q}$, että jokaisella a_n on tämä ominaisuus ja $N \geq 1/\epsilon$. Tällöin $2 < a_n^2 < 2 + \epsilon$ kaikilla $n > N$ ja näin ollen $|a_n^2 - 2| < \epsilon$ kaikilla $n > N$. Tästä johtuen $a_n^2 \to 2$ kun $n \to \infty$. □

Lause 5.1.6. *Jono (a_n) joka toteuttaa Lemman 5.1.5 on Cauchyn jono.*

Todistus. Oletetaan, että (a_n) ei ole Cauchyn jono. Tällöin on olemassa $\epsilon > 0$, siten että kaikilla $N \in \mathbb{N}$ on olemassa luonnolliset luvut n, m, jotka ovat suurempia kuin N ja joille pätee $|a_n - a_m| \geq \epsilon$. Olkoon n ja m tällaiset luvut. Tällöin

$$|a_n^2 - a_m^2| = |(a_n - a_m)(a_n + a_m)| = |a_n - a_m||a_n + a_m| \geq \epsilon(a_n + a_m) > 2\epsilon$$

sillä $a_n > 1$ ja $a_m > 1$.

Lemma 5.1.5 osoittaa, että jono (a_n^2) suppenee ja siten Lauseen 5.1.4 mukaan sen on oltava Cauchyn jono. Tästä johtuen on olemassa $N_1 \in \mathbb{N}$ siten, että epäyhtälö $|a_k^2 - a_j^2| < 2\epsilon$ toteutuu kaikilla $k > N_1$ ja $j > N_1$. Toisaalta millä tahansa $N \in \mathbb{N}$ on todettu sellaisen parin n, m olemassa olo, jolle pätee $n > N, m > N$ ja $|a_n^2 - a_m^2| > 2\epsilon$. Tämän ristiriidan myötä voidaan todeta, että (a_n) on Cauchyn jono. □

Merkitään kaikkien joukon $\mathbb{Q}$ Cauchyn jonojen joukkoa merkinnällä $\mathbb{Q}^c$. Kahden joukon $\mathbb{Q}^c$ jonon (a_n) ja (b_n) sanotaan olevan ekvivalentteja, jos jokaisella positiivisella rationaaliluvulla ϵ on olemassa luonnollinen luku N siten, että $|a_n - b_n| < \epsilon$ kaikilla $n > N$. Merkitään $(a_n) \sim (b_n)$ kun tämä pätee. On huomattava, että $(a_n) \sim (b_n)$ jos ja vain jos $(a_n - b_n) \sim (0)$.

Lause 5.1.7. *Relaatio $\sim$ on ekvivalenssirelaatio joukossa $\mathbb{Q}^c$.*

Todistus. Nähdään suoraan relaation määritelmästä, että $(a_n) \sim (a_n)$ kaikilla $(a_n) \in \mathbb{Q}^c$. Näin ollen relaatio on refleksiivinen. Koska $|a_n - b_n| = |b_n - a_n|$, on selvää, että $(a_n) \sim (b_n)$ merkitsee sitä, että $(b_n) \sim (a_n)$ kaikilla $(a_n), (b_n) \in \mathbb{Q}^c$. Siten symmetrisyys on osoitettu.

Täytyy vielä osoittaa, että relaatio on transitiivinen. Oletetaan, että $(a_n) \sim (b_n)$ ja $(b_n) \sim (c_n)$ kaikilla $(a_n), (b_n), (c_n) \in \mathbb{Q}^c$. Täytyy osoittaa, että millä tahansa $\epsilon > 0$ on olemassa sellainen N jolle $|a_n - c_n| < \epsilon$ kaikilla $n > N$. Valitaan $\epsilon > 0$, kolmioepäyhtälöstä saadaan

$$|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n|.$$

Koska $(a_n) \sim (b_n)$, on olemassa N_1 siten, että $|a_n - b_n| < \epsilon/2$ kaikilla $n > N_1$. Samoin, koska $(b_n) \sim (c_n)$, on olemassa N_2 siten, että $|b_n - c_n| < \epsilon/2$ kaikilla $n > N_2$. Valitsemalla $N = \max\{N_1, N_2\}$ nähdään, että $|a_n - c_n| < \epsilon/2 + \epsilon/2 = \epsilon$, kaikilla $n > N$ ja niin $(a_n) \sim (c_n)$. Täten myös transitiivisuus on osoitettu ja relaatio on ekvivalenssirelaatio. □

Merkinnällä $[\mathbb{Q}^c]$ tarkoitetaan kaikkien ekvivalenssiluokkien joukkoa relaatiossa $\sim$. Joukossa $[\mathbb{Q}^c]$ osa ekvivalenssiluokista on rationaalisia vakiojonoja. Lauseesta 5.1.4 seuraa, että jokainen suppeneva jono joukossa $\mathbb{Q}$ kuuluu luokkaan, jonka edustaja on vakiojono. Toisaalta on olemassa vähintään yksi ekvivalenssiluokka, jolla ei ole tällaista edustajaa. Joukko $[\mathbb{Q}^c]$ voidaan tästä johtuen jakaa kahteen epätyhjään joukkoon

(1) $\mathbb{R}_\mathbb{Q} = \{[a] : a \in \mathbb{Q}\}$;

(2) $\mathbb{R}_I = [\mathbb{Q}^c] - \mathbb{R}_\mathbb{Q}$.

Joukon $\mathbb{R}_I$ alkioita kutsutaan *irrationaaliluvuiksi*. Olkoon $\mathbb{R} = \mathbb{R}_\mathbb{Q} \cup \mathbb{R}_I = [\mathbb{Q}^c]$ ja alkioita $[0]$ ja $[1]$ merkitään 0 ja 1. Yhteenlaskun ja kertolaskun indusoituja laskutoimituksia merkitään $+$ ja $\cdot$. Toisin sanoen määritämme $[(a_n)] + [(b_n)] = [(a_n + b_n)]$ ja $[(a_n)][(b_n)] = [(a_n b_n)]$

Määritellään $\Phi(a) = [a]$ kun $a \in \mathbb{Q}$. Tällöin Φ on bijektio joukosta $\mathbb{Q}$ joukkoon $\mathbb{R}_\mathbb{Q}$. Lisäksi, jos $(a, b) \in \mathbb{Q} \times \mathbb{Q}$, niin

$$\Phi(a) + \Phi(b) = [a] + [b] = [a + b] = \Phi(a + b).$$

Vastaavasti

$$\Phi(a)\Phi(b) = \Phi(ab).$$

Näin ollen $\mathbb{R}_\mathbb{Q}$ voidaan samaistaa joukoksi $\mathbb{Q}$. Erityisesti on huomattava, että $\Phi(0) = [0]$ ja samoin $\Phi(1) = [1]$. Täten 0 ja 1 joukossa $\mathbb{R}$ on sovitettu vastaavien rationaalilukujen kanssa. Voimme nyt kirjoittaa a ilmaisun $[a]$ sijaan kun $a \in \mathbb{Q}$.

Lause 5.1.8. $(\mathbb{R}, +, \cdot, 0, 1)$ *on vaihdannainen rengas jolla on neutraalialkio.*

Todistus. Väite seuraa siitä, että $(\mathbb{Q}, +, \cdot, 0, 1)$ on vaihdannainen rengas. Lisäksi perusteluina ovat laskutoimitusten $+$ ja $\cdot$ määritelmät sekä se, että 0 ja 1 ovat toisistaan eroavia rationaalilukuja.

Esimerkiksi

$$[(a_n)] + [(b_n)] = [(a_n + b_n)] = [(b_n + a_n)] = [(b_n)] + [(a_n)].$$

On huomattava, että $-[(a_b)] + [(-a_n)] = [(a_n - a_n)] = [0] = 0$, eli $-[(a_n)] = [(-a_n)]$. Muiden ehtojen todistukset ovat vastaavanlaisia ja ohitamme ne tässä yhteydessä. □

Nyt voimme osoittaa, että $x^2 = 2$ voidaan ratkaista reaalilukujen järjestelmässä.

Lause 5.1.9. *On olemassa* $x \in \mathbb{R}$ *jolla* $x^2 = 2$.

Todistus. Lauseiden 5.1.5 ja 5.1.6 mukaan on olemassa Cauchyn jono (a_n) joukossa $\mathbb{Q}$ jolle $a_n^2 \to 2$ kun $n \to \infty$. Olkoon $x = |(a_n)|$. Tällöin

$$x^2 = |(a_n)|^2 = |(a_n^2)| = |2| = 2.$$

□

Epäilemättä, mikä tahansa yhtälön $x^2 = 2$ ratkaisu on irrationaaliluku.

Lause 5.1.10. *Oletetaan, että* $[(a_n)] \neq 0$. *Tällöin on olemassa positiivinen rationaaliluku* λ *ja luonnollinen luku* N, *joille pätee* $|a_n| > \lambda$ *kaikilla* $n > N$.

Todistus. Oletetaan, että lause ei päde jollakin Cauchyn jonolla (a_n) jolle $[(a_n)] \neq 0$. Tällöin jokaisella rationaalisella $\lambda > 0$ ja jokaisella $N \in \mathbb{N}$ on olemassa $n > N$ siten, että $|a_n| \leq \lambda$. Edetään ristiriitaan todistamalla, että $a_n \to 0$. Valitaan $\epsilon > 0$. Koska $(a_n) \in \mathbb{Q}^c$, on olemassa $N \in \mathbb{N}$ siten, että $|a_n - a_m| < \epsilon/2$ kun $m, n > N$. Kolmioepäyhtälöstä seuraa

$$|a_n| = |a_m + a_n - a_m| \leq |a_m| + |a_n - a_m| < |a_m| + \epsilon/2$$

kun $m, n > N$. Valitaan $m > N$ siten, että $|a_m| \leq \epsilon/2$ (valitsemalla $\lambda = \epsilon/2$ edellisessä kohdassa). Tällöin $|a_n| < \epsilon/2 + \epsilon/2 = \epsilon$ kaikilla $n > N$. Näin ollen $a_n \to 0$ kun $n \to \infty$, joka on ristiriidassa oletuksen $[(a_n)] \neq 0$ kanssa. □

Nollajono on mikä tahansa luokan [0] jono. Edellinen lause osoittaa, että jos (a_n) ei ole nollajono se voidaan rajata pois nollasta. Toisin sanoen on olemassa positiivinen alaraja jonolle $|a_n|$, kun n on riittävän suuri. Tätä tulosta voidaan käyttää todistamaan käänteisluvun olemassaolo ja siten jakolasku voidaan määrittää joukossa $\mathbb{R} \setminus \{0\}$.

Lause 5.1.11. *Jos* $s = [(a_n)] \in \mathbb{R} \setminus \{0\}$, *on olemassa* $r \in \mathbb{R}$ *siten, että* $rs = 1$.

Todistus. Oletetaan, että $s = [(a_n)] \in \mathbb{R}\setminus\{0\}$. Tällöin Lauseen 5.1.10 mukaan on olemassa positiivinen rationaaliluku λ ja luonnollinen luku N_1 siten, että $|a_n| > \lambda$ kun $n > N_1$. Tästä johtuen kaikilla arvoilla $n > N_1$ on jokaisella a_n olemassa käänteisalkio $1/a_n \in \mathbb{Q}$. On huomattava, että

$$\frac{1}{a_n} \leq \frac{1}{|a_n|} < \frac{1}{\lambda}.$$

Määritellään jono (b_n) asettamalla $b_n = 1$ kaikilla $n \leq N_1$ ja $b_n = 1/a_n$ kaikilla $n > N_1$. Kaikilla m ja n jotka ovat suurempia kuin N_1 pätee

$$|b_n - b_m| = |\frac{1}{a_n} - \frac{1}{a_m}| = \frac{1}{|a_n||a_m|}|a_m - a_n| \leq \frac{|a_m - a_n|}{\lambda^2}.$$

Koska $(a_n) \in \mathbb{Q}^c$ kaikilla $\epsilon > 0$, on olemassa N_2 siten, että $|a_m - a_n| < \lambda^2\epsilon$ kun $m, n > N_2$. Olkoon $N = \max\{N_1, N_2\}$. Tällöin $|b_n - b_m| < \epsilon$ kun $m > N$ ja $n > N$, siten (b_n) on Cauchyn jono. Olkoon $r = [(b_n)]$. Tällöin, $rs = [(a_n)][(b_n)] = [(a_n b_n)] = [1] = 1$. □

Edellisistä lauseista seuraa, että $(\mathbb{R}, +, \cdot, 0, 1)$ on kunta. Voimme nyt käyttää edellisen luvun yleistyksiä, esimerkiksi potenssiin korotukseen laskusääntöjä. Tässä tapauksessa $r^n = \prod_{k=1}^{n} r$ kaikilla $r \in \mathbb{R}$ ja $n \in \mathbb{N}$, yhtäpitävänä aiemman potenssiin korotuksen määritelmän kanssa. Määritetään myös $r^0 = 1$ jos $r \in \mathbb{R} \setminus \{0\}$.

Edellisten lukujärjestelmien muodostamisen tapaan, seuraava askel on yleistää järjestysrelaation käsite. Jos rationaaliluvuille a ja b pätee $a < b$, laajennuksen myötä on saatava $[a] < [b]$ eli positiivisten lukujen käsitekin on laajennettava. Jono $(a_n) \in \mathbb{Q}^c$ on positiivinen jos on olemassa positiivinen rationaaliluku ϵ ja luonnollinen luku $N \in \mathbb{N}$ niin, että $a_n > \epsilon$ pätee kaikilla $n > N$. On huomattava, että vakiojono (a_n) on positiivinen jos ja vain jos $a > 0$. Seuraava lause osoittaa, että positiivisuus leimaa koko ekvivalenssiluokan joka liittyy positiiviseen jonoon.

Lause 5.1.12. *Jos* $(a_n) \in \mathbb{Q}^c$ *on positiivinen, niin jokainen* $(b_n) \in [(a_n)]$ *on myös positiivinen.*

Todistus. Oletetaan, että (a_n) on positiivinen ja $(b_n) \sim (a_n)$. Koska (a_n) on positiivinen, on olemassa positiivinen rationaaliluku ϵ ja luonnollinen luku N_1 siten, että $a_n > \epsilon$ kaikilla $n > N_1$. Koska $(b_n) \sim (a_n)$, on olemassa luonnollinen luku N_2 siten, että $|a_n - b_n| < \epsilon/2$, kun $n > N_2$. Olkoon $N = \max\{N_1, N_2\}$. Kaikilla $n > N$ pätee $a_n - b_n < \epsilon/2$ ja niin $b_n > a_n - \epsilon/2 > \epsilon - \epsilon/2 = \epsilon/2 > 0$. Näin ollen (b_n) on positiivinen. □

Lause 5.1.13. *Olkoon* $(a_n) \in \mathbb{Q}^c$ *ja* $(b_n) \in \mathbb{Q}^c$ *positiivisia jonoja. Tällöin jonot* $(a_n + b_n)$ *ja* $(a_n b_n)$ *ovat positiivisia.*

Todistus. Koska (a_n) on positiivinen, on olemassa positiivinen rationaaliluku ϵ_1 ja $N_1 \in \mathbb{N}$ joilla pätee $a_n > \epsilon_1$ kaikilla $n > N_1$. Vastaavasti on olemassa positiivinen rationaaliluku ϵ_2 ja $N_2 \in \mathbb{N}$ joilla pätee $b_n > \epsilon_2$ kaikilla $n > N_2$. Olkoon $N = \max\{N_1, N_2\}$, ja valitaan $n > N$. Koska $n > N_1$, pätee $a_n > \epsilon_1$. Vastaavasti $b_n > \epsilon_2$ ja siten $a_n + b_n > \epsilon_1 + \epsilon_2 > 0$ sekä $a_n b_n > \epsilon_1 \epsilon_2 > 0$. Näin ollen $(a_n + b_n)$ ja $(a_n b_n)$ ovat positiivisia. □

Lause 5.1.14. *Jokaiselle jonolle* $(a_n) \in \mathbb{Q}^c$ *pätee tasan yksi seuraavista väittämistä:*

(a) (a_n) *on positiivinen*

(b) (a_n) *on nollajono*

(c) $(-a_n)$ *on positiivinen*

Todistus. Oletetaan, että (a_n) on nollasta poikkeava. On olemassa rationaaliluku ϵ ja $N_1 \in \mathbb{N}$ niin, että $|a_n| > \epsilon$ kaikilla $n > N_1$. Täten joko $a_n > \epsilon$ tai $-a_n > \epsilon$ kaikilla $n > N_1$. Cauchyn jonon ominaisuuksien mukaan on olemassa $N_2 \in \mathbb{N}$ siten, että $|a_n - a_m| < \epsilon$ kun $n > N_2$ ja $m > N_2$. Olkoon $N = \max\{N_1, N_2\}$. Jos on olemassa $m, n \geq N$ siten, että $a_n > \epsilon$ ja $-a_n > \epsilon$, niin $a_n - a_m > 2\epsilon$, joka on ristiriidassa Cauchyn jonon määrittelyn kanssa. Seuraa, että joko $a_n > \epsilon$ kun $n > N$ tai $-a_n > \epsilon$ kun $n > N$. Toisin sanoen joko (a_n) tai $(-a_n)$ on positiivinen.

Päättelemme, että ainakin yksi väittämistä (a), (b) tai (c) pätee. Seuraavaksi oletetaan, että (a_n) on nolla. Jokaisella rationaaliluvulla ϵ on olemassa $N \in \mathbb{N}$ siten, että $|a_n| < \epsilon$ kaikilla $n > N$. Näin ollen (a_n) ei voi olla positiivinen. Myöskään $(-a_n)$ ei voi olla positiivinen, sillä jos $-a > \epsilon > 0$, niin $|a_n| > \epsilon$.

Pitäisi vielä osoittaa, että molemmat jonoista (a_n) ja $(-a_n)$ eivät voi olla positiivisia. Jos (a_n) on positiivinen, niin jollakin rationaaliluvulla ϵ_1 ja $N_1 \in \mathbb{N}$ pätee $a_n > \epsilon_1$ kun $n > N_1$. Jos $(-a_n)$ on myös positiivinen, niin jollakin positiivisella rationaaliluvulla ϵ_2 ja $N_2 \in \mathbb{N}$ pätee $-a_n > \epsilon_2$ kun $n > N_2$. Olkoon $\epsilon = \min\{\epsilon_1, \epsilon_2\}$ ja $N = \max\{N_1, N_2\}$ sekä valitaan $n > N$. Tällöin $n > N_1$ ja siten $a_n > \epsilon_1 \geq \epsilon > 0 > -a_n$. Vastaavasti $n > N_2$ ja päädytään ristiriitaan, että $-a_n > \epsilon_2 \geq \epsilon$. □

Edeltävät lauseet tarkoittavat sitä, että jonon positiivisuudessa on itseasiassa kyse ekvivalenssiluokan, johon kyseinen jono kuuluu, positiivisuudesta. Tämä seikka mahdollistaa myös positiivisen ekvivalenssiluokan määrittelyn.

Tarkemmin sanottuna $[(a_n)]$ on positiivinen, jos (a_n) on positiivinen. Toisaalta $[(a_n)]$ on negatiivinen, jos $(-a_n)$ on positiivinen.

Relaatio $<$ määritellään joukossa $\mathbb{R}$ seuraavasti. Kirjoitamme $[(a_n)] < [(b_n)]$ tai $[(b_n)] > [(a_n)]$ jos $[(b_n - a_n)]$ on positiivinen. Jos a ja b ovat rationaalilukuja joille pätee $a < b$, niin $b - a > 0$ ja niin $(b - a)$ on positiivinen jono ja $[a] < [b]$. Tämä pätee myös kääntäen, eli $[a] < [b]$ jos ja vain jos $a < b$. On huomattava myös, että $[(a_n)] > 0$ jos ja vain jos $[(a_n)]$ on positiivinen ja tästä johtuen $[(a_n)] < [(b_n)]$ jos ja vain jos $[(b_n)] - [(a_n)] = [(b_n - a_n)] > 0$. Vastaavasti $[(a_n)] < 0$ jos ja vain jos $[(a_n)]$ on negatiivinen ja $[(a_n)] > [(b_n)]$ jos ja vain jos $[(a_n)] - [(b_n)] > 0$.

Jos $r, s \in \mathbb{R}$ ja $r < s$, niin luvun r sanotaan olevan pienempi kuin s ja luvun s sanotaan olevan suurempi kuin r, sovussa termien aiempien käyttötapojen kanssa. Kirjoitamme myös $r \leq s$ tai $s \geq r$ jos joko $r < s$ tai $r = s$. Näin ollen $[(a_n)] \geq 0$ jos on olemassa $N \in \mathbb{N}$ niin, että $a_n \geq 0$ kaikilla $n > N$.

Nyt voimme vahvistaa, että $(\mathbb{R}, +, \cdot, 0, 1, <)$ on järjestetty kokonaisalue. Järjestetyn kokonaisalueen määritelmän ehdot voidaan tarkastaa samaan tapaan kuin edellä tehtiin kokonaislukujen ja rationaalilukujen tapauksessa. Koska $(\mathbb{R}, +, \cdot, 0, 1)$ on kunta, $(\mathbb{R}, +, \cdot, 0, 1, <)$ on järjestetty kunta. Tätä järjestettyä kuntaa kutsutaan reaalilukujen järjestelmäksi.

Reaaliluvut on mahdollista määritellä myös toisilla tavoilla. Esimerkiksi Dedekind määritteli reaaliluvut tekemällä leikkauksia rationaalilukujen joukossa. Tällaisia leikkauksia ja reaalilukujen määrittelytapaa kutsutaan Dedekindin leikkauksiksi. Lisää tästä ja muista reaalilukujen määrittelytavoista voi lukea esimerkiksi teoksista [6] ja [3].

Viitteet

[1] Graham, M. *Modern Elementary Mathematics.* Harcourt Brace Jovanovich, Inc., New York, 1970.

[2] Hrbacek, K. , Jech, K. *Introduction to set theory, 3ed.* Marcel Dekker, Inc., New York, 1999.

[3] Ebbinghaus , H.-D. *Numbers.* Springer, New York, 1995.

[4] Little, C. H. C. *Number systems of analysis* , World Scientific, Singapore, 2003.

[5] Irving, R. S. *Integers, polynomials, and rings : a course in algebra*, Springer, New York, 2004.

[6] Artmann, B. *Concept of number : from quaternions to monads and topological fields*, Ellis Horwood, Chichester, 1988.